Catalyst 2900 Series XL and Catalyst 3500 Series XL Software Configuration Guide

Cisco IOS Release 12.0(5)WC3
January 2002

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC-786511=
Text Part Number: 78-6511-06

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

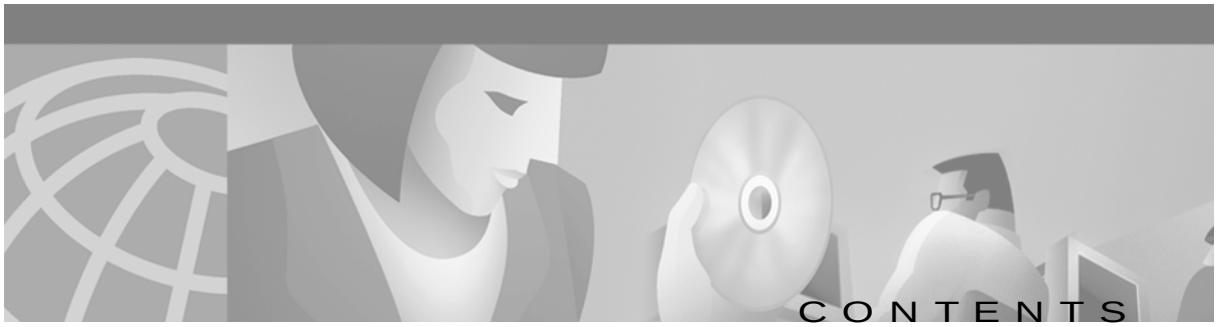
NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

AccessPath, AtmDirector, Browse with Me, CCIP, CCSI, CD-PAC, *CiscoLink*, the Cisco *Powered* Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Cisco Unity, Fast Step, Follow Me Browsing, FormShare, FrameShare, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, ScriptBuilder, ScriptShare, SMARTnet, TransPath, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and Discover All That's Possible are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, GigaStack, IOS, IP/TV, LightStream, MICA, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0110R)

Catalyst 2900 Series XL and Catalyst 3500 Series XL Software Configuration Guide
Copyright © 1998-2002, Cisco Systems, Inc.
All rights reserved.



Preface xiii

Audience xiii

Purpose xiii

Organization xiv

Conventions xv

Related Publications xvi

Obtaining Documentation xvii

World Wide Web xvii

Cisco Documentation CD-ROM xvii

Ordering Documentation xvii

Registered Cisco Direct Customers xvii

Non-Registered Cisco.com Users xvii

Documentation Feedback xviii

Obtaining Technical Assistance xviii

Cisco.com xviii

Technical Assistance Center xix

Contacting TAC by Using the Cisco TAC Website xix

Contacting TAC by Telephone xix

CHAPTER 1

Overview 1-1

Features 1-1

Management Options 1-5

Management Interface Options 1-5

Advantages of Using CMS and Clustering Switches 1-6

Network Configuration Examples 1-7

Design Concepts for Using the Switch 1-7

Small to Medium-Sized Network Configuration 1-10

Collapsed Backbone and Switch Cluster Configuration 1-12

Large Campus Configuration 1-14

Multidwelling Configuration 1-16

CHAPTER 2 **Getting Started with CMS** 2-1

Features 2-2

Front Panel View 2-4

Cluster Tree 2-5

Front-Panel Images 2-6

Redundant Power System LED 2-7

Port Modes and LEDs 2-8

VLAN Membership Modes 2-12

Topology View 2-13

Topology Icons 2-15

Device and Link Labels 2-16

Colors in the Topology View 2-17

Topology Display Options 2-17

Menus and Toolbar 2-18

Menu Bar 2-18

Toolbar 2-23

Front Panel View Popup Menus 2-24

Device Popup Menu 2-24

Port Popup Menu 2-24

Topology View Popup Menus 2-25

Link Popup Menu 2-25

Device Popup Menus 2-26

Interaction Modes 2-28

Guide Mode 2-28

Expert Mode 2-28

Wizards 2-28

Tool Tips 2-29

Online Help 2-29

CMS Window Components 2-30

Host Name List 2-30

Tabs, Lists, and Tables 2-31

Icons Used in Windows 2-31

Buttons 2-31

Accessing CMS 2-32

Access Modes in CMS 2-33

Verifying Your Changes 2-34

Change Notification 2-34

Error Checking 2-34

Saving Your Changes 2-34
Using Different Versions of CMS 2-35
Where to Go Next 2-35

CHAPTER 3 **Getting Started with the CLI 3-1**
Command Usage Basics 3-2
Accessing Command Modes 3-2
Specifying Ports in Interface Configuration Mode 3-4
Abbreviating Commands 3-4
Using the No and Default Forms of Commands 3-5
Redisplaying a Command 3-5
Getting Help 3-5
Command-Line Error Messages 3-6
Accessing the CLI 3-7
Accessing the CLI from a Browser 3-7
Saving Configuration Changes 3-8
Where to Go Next 3-8

CHAPTER 4 **General Switch Administration 4-1**
Basic IP Connectivity to the Switch 4-2
Switch Software Releases 4-2
Console Port Access 4-3
Telnet Access to the CLI 4-4
HTTP Access to CMS 4-5
SNMP Network Management Platforms 4-5
Using FTP to Access the MIB Files 4-6
Using SNMP to Access MIB Variables 4-6
Default Settings 4-8

CHAPTER 5 **Clustering Switches 5-1**
Understanding Switch Clusters 5-2
Command Switch Characteristics 5-2
Standby Command Switch Characteristics 5-3
Candidate and Member Switches Characteristics 5-3
Planning a Switch Cluster 5-4
Automatic Discovery of Cluster Candidates and Members 5-4
Discovery through CDP Hops 5-5
Discovery through Non-CDP-Capable and Noncluster-Capable Devices 5-6

Discovery through the Same Management VLAN 5-7
Discovery through Different Management VLANs 5-8
Discovery of Newly Installed Switches 5-9
HSRP and Standby Command Switches 5-10
Virtual IP Addresses 5-11
Automatic Recovery of Cluster Configuration 5-11
Considerations for Cluster Standby Groups 5-12
IP Addresses 5-13
Host Names 5-14
Passwords 5-14
SNMP Community Strings 5-14
TACACS+ 5-15
Access Modes in CMS 5-15
Management VLAN 5-16
Network Port 5-16
NAT Commands 5-17
LRE Profiles 5-17
Availability of Switch-Specific Features in Switch Clusters 5-17
Creating a Switch Cluster 5-17
Enabling a Command Switch 5-18
Adding Member Switches 5-19
Creating a Cluster Standby Group 5-21
Verifying a Switch Cluster 5-23
Using the CLI to Manage Switch Clusters 5-24
Catalyst 1900 and Catalyst 2820 CLI Considerations 5-24
Using SNMP to Manage Switch Clusters 5-25

CHAPTER 6 **Configuring the System** 6-1
Changing IP Information 6-2
Manually Assigning and Removing Switch IP Information 6-2
Using DHCP-Based Autoconfiguration 6-3
Understanding DHCP-Based Autoconfiguration 6-3
DHCP Client Request Process 6-4
Configuring the DHCP Server 6-5
Configuring the TFTP Server 6-5
Configuring the Domain Name and the DNS 6-6
Configuring the Relay Device 6-7
Obtaining Configuration Files 6-8
Example Configuration 6-9

Assigning Passwords and Privilege Levels 6-11
Setting the System Date and Time 6-12
Configuring Daylight Saving Time 6-12
Configuring the Network Time Protocol 6-13
Configuring the Switch as an NTP Client 6-13
Enabling NTP Authentication 6-13
Configuring the Switch for NTP Broadcast-Client Mode 6-13
Configuring CDP 6-13
Configuring CDP for Extended Discovery 6-14
Managing the MAC Address Tables 6-15
MAC Addresses and VLANs 6-15
Changing the Address Aging Time 6-16
Removing Dynamic Address Entries 6-16
MAC Address Notification 6-17
Adding Secure Addresses 6-18
Removing Secure Addresses 6-18
Adding Static Addresses 6-19
Removing Static Addresses 6-19
Configuring Static Addresses for EtherChannel Port Groups 6-20
Configuring CGMP 6-20
Enabling the Fast Leave Feature 6-21
Disabling the CGMP Fast Leave Feature 6-21
Changing the CGMP Router Hold-Time 6-22
Removing Multicast Groups 6-22
Configuring IGMP Filtering 6-23
Configuring IGMP Profiles 6-23
Applying IGMP Filters 6-25
Setting the Maximum Number of IGMP Groups 6-26
Configuring MVR 6-27
Using MVR in a Multicast Television Application 6-27
Configuration Guidelines and Limitations 6-29
Setting MVR Parameters 6-30
Configuring MVR 6-31
Managing the ARP Table 6-32
Configuring STP 6-33
Supported STP Instances 6-33
Using STP to Support Redundant Connectivity 6-34
Disabling STP 6-34
Accelerating Aging to Retain Connectivity 6-34

Configuring STP and UplinkFast in a Cascaded Cluster 6-35
Configuring Redundant Links By Using STP UplinkFast 6-36
Enabling STP UplinkFast 6-37
Configuring Cross-Stack UplinkFast 6-37
How CSUF Works 6-37
Events that Cause Fast Convergence 6-39
Limitations 6-39
Connecting the Stack Ports 6-40
Configuring Cross-Stack UplinkFast 6-41
Changing the STP Parameters for a VLAN 6-42
Changing the STP Implementation 6-42
Changing the Switch Priority 6-43
Changing the BPDU Message Interval 6-43
Changing the Hello BPDU Interval 6-44
Changing the Forwarding Delay Time 6-44
STP Port States 6-45
Enabling the Port Fast Feature 6-45
Changing the Path Cost 6-46
Changing the Port Priority 6-46
Configuring STP Root Guard 6-47
Configuring SNMP 6-48
Disabling and Enabling SNMP 6-48
Entering Community Strings 6-49
Adding Trap Managers 6-49
Configuring TACACS+ 6-51
Configuring the TACACS+ Server Host 6-51
Configuring Login Authentication 6-52
Specifying TACACS+ Authorization for EXEC Access and Network Services 6-53
Starting TACACS+ Accounting 6-54
Configuring a Switch for Local AAA 6-54

CHAPTER 7 **Configuring the Switch Ports** 7-1
Changing the Port Speed and Duplex Mode 7-2
Connecting to Devices That Do Not Autonegotiate 7-2
Setting Speed and Duplex Parameters 7-3
Configuring Flow Control on Gigabit Ethernet Ports 7-3
Configuring Flooding Controls 7-4
Enabling Storm Control 7-4
Disabling Storm Control 7-5

Blocking Flooded Traffic on a Port 7-5
Resuming Normal Forwarding on a Port 7-6
Enabling a Network Port 7-6
Disabling a Network Port 7-7
Configuring UniDirectional Link Detection 7-7
Creating EtherChannel Port Groups 7-8
Understanding EtherChannel Port Grouping 7-8
Port Group Restrictions on Static-Address Forwarding 7-9
Creating EtherChannel Port Groups 7-9
Configuring Protected Ports 7-10
Enabling Port Security 7-11
Defining the Maximum Secure Address Count 7-12
Enabling Port Security 7-12
Disabling Port Security 7-12
Configuring SPAN 7-13
Enabling SPAN 7-13
Disabling SPAN 7-13
Configuring Voice Ports 7-14
Preparing a Port for a Cisco 7960 IP Phone Connection 7-14
Configuring a Port to Connect to a Cisco 7960 IP Phone 7-15
Overriding the CoS Priority of Incoming Frames 7-15
Configuring Voice Ports to Carry Voice and Data Traffic on Different VLANs 7-16
Configuring Inline Power on the Catalyst 3524-PWR Ports 7-17

CHAPTER 8 **Configuring VLANs 8-1**
Overview 8-2
Management VLANs 8-3
Changing the Management VLAN for a New Switch 8-4
Changing the Management VLAN Through a Telnet Connection 8-4
Assigning VLAN Port Membership Modes 8-5
VLAN Membership Combinations 8-6
Assigning Static-Access Ports to a VLAN 8-7
Overlapping VLANs and Multi-VLAN Ports 8-7
Using VTP 8-9
The VTP Domain 8-9
VTP Modes and Mode Transitions 8-10
VTP Advertisements 8-11
VTP Version 2 8-11

VTP Pruning 8-12
VTP Configuration Guidelines 8-13
Domain Names 8-13
Passwords 8-13
Upgrading from Previous Software Releases 8-13
VTP Version 8-14
Default VTP Configuration 8-14
Configuring VTP 8-15
Configuring VTP Server Mode 8-15
Configuring VTP Client Mode 8-16
Disabling VTP (VTP Transparent Mode) 8-17
Enabling VTP Version 2 8-17
Disabling VTP Version 2 8-18
Enabling VTP Pruning 8-18
Monitoring VTP 8-19
VLANs in the VTP Database 8-19
Token Ring VLANs 8-19
VLAN Configuration Guidelines 8-20
Default VLAN Configuration 8-20
Configuring VLANs in the VTP Database 8-22
Adding a VLAN 8-23
Modifying a VLAN 8-23
Deleting a VLAN from the Database 8-24
Assigning Static-Access Ports to a VLAN 8-24
How VLAN Trunks Work 8-25
IEEE 802.1Q Configuration Considerations 8-25
Trunks Interacting with Other Features 8-26
Configuring a Trunk Port 8-27
Disabling a Trunk Port 8-28
Defining the Allowed VLANs on a Trunk 8-28
Changing the Pruning-Eligible List 8-29
Configuring the Native VLAN for Untagged Traffic 8-29
Configuring 802.1p Class of Service 8-30
How Class of Service Works 8-30
Port Priority 8-30
Port Scheduling 8-30
Configuring the CoS Port Priorities 8-31

Load Sharing Using STP 8-31
Load Sharing Using STP Port Priorities 8-31
Configuring STP Port Priorities and Load Sharing 8-32
Load Sharing Using STP Path Cost 8-33
How the VMPS Works 8-35
Dynamic Port VLAN Membership 8-35
VMPS Database Configuration File 8-36
VMPS Configuration Guidelines 8-37
Default VMPS Configuration 8-38
Configuring Dynamic VLAN Membership 8-38
Configuring Dynamic Ports on VMPS Clients 8-39
Reconfirming VLAN Memberships 8-39
Changing the Reconfirmation Interval 8-40
Changing the Retry Count 8-40
Administering and Monitoring the VMPS 8-41
Troubleshooting Dynamic Port VLAN Membership 8-41
Dynamic Port VLAN Membership Configuration Example 8-41

CHAPTER 9 **Troubleshooting** 9-1
Avoiding Configuration Conflicts 9-2
Avoiding Autonegotiation Mismatches 9-3
Troubleshooting CMS Sessions 9-4
Determining Why a Switch Is Not Added to a Cluster 9-7
Copying Configuration Files to Troubleshoot Configuration Problems 9-8
Troubleshooting Switch Software Upgrades 9-9
Recovery Procedures 9-11
Recovering from Lost Member Connectivity 9-11
Recovering from a Command Switch Failure 9-11
Replacing a Failed Command Switch with a Cluster Member 9-12
Replacing a Failed Command Switch with Another Switch 9-14
Recovering from a Failed Command Switch Without Replacing the Command Switch 9-16
Recovering from a Lost or Forgotten Password 9-17
Recovering from Corrupted Software 9-19

APPENDIX A

System Messages A-1

Overview A-1

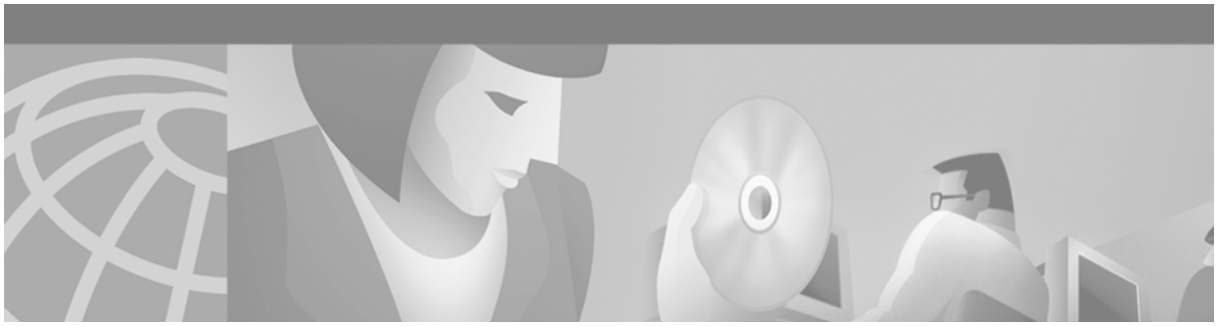
How to Read System Messages A-2

Error Message Traceback Reports A-4

Error Message and Recovery Procedures A-4

AAAA Messages A-5
CAPITOLA Messages A-7
CDP Messages A-7
CHASSIS Message A-8
CMP Messages A-8
CPU_NET Message A-9
ENVIRONMENT Messages A-9
FRANK Messages A-10
GBIC_1000BASET Messages A-15
GigaStack Messages A-16
HW_MEMORY Messages A-17
INTERFACE Messages A-18
IP Messages A-18
MAT Messages A-19
MIRROR Messages A-20
MODULES Messages A-20
PERF5_HALT_MSG Message A-21
PM Messages A-22
PMSM Messages A-24
PORT_SECURITY Messages A-25
PRUNING Messages A-25
RAC Message A-29
REGISTORS Messages A-29
RTD Messages A-30
SNMP Messages A-31
SPANTREE Messages A-31
SPANTREE_FAST Messages A-34
STORM_CONTROL Message Messages A-35
SW_VLAN Messages A-35
SYS Messages A-37
TAC Messages A-40
TTYDRIVER Messages A-41
VQPCLIENT Messages A-42
VTP Message A-45

INDEX



Preface

Audience

The *Catalyst 2900 Series XL and Catalyst 3500 Series XL Software Configuration Guide* is for the network manager responsible for configuring the Catalyst 2900 series XL and Catalyst 3500 series XL switches, hereafter referred to as the switches. Before using this guide, you should be familiar with the concepts and terminology of Ethernet and local area networking.

Purpose

Note This switch software release is based on Cisco IOS Release 12.0. It has been enhanced to support a set of features for the Catalyst 2900 XL and Catalyst 3500 XL switches. This guide does not repeat the concepts and CLI procedures already documented in the Cisco IOS Release 12.0 documentation on Cisco.com.

Note This guide describes the features for the Catalyst 2900 XL and Catalyst 3500 XL switches that are *not* Long-Reach Ethernet (LRE) switches. The Cisco IOS Release 12.0(5)WC3 software is for non-LRE switches only. Do not install this release on the Catalyst 2900 LRE XL switches. For configuring the Catalyst 2900 LRE XL switches, refer to Cisco IOS Release 12.0(5)WC2.

This guide provides information about configuring and troubleshooting a switch or switch clusters. It includes descriptions of the management interface options and the features supported by the switch software.

For the following topics, use this guide with other documents:

- Requirements—This guide assumes you have met the hardware and software requirements and cluster compatibility requirements that are described in the release notes.
- Start up information—This guide assumes you have initially configured the switch by using the setup program, as described in the release notes.
- Cluster Management Suite (CMS) information—This guide provides an overview of the CMS web-based, switch management interface. For information about CMS requirements and the procedures for browser and plug-in configuration and accessing CMS, refer to the release notes. For CMS field-level window descriptions and procedures, refer to the CMS online help.

- Cluster configuration—This guide provides information about planning for, creating, and maintaining switch clusters. Because configuring switch clusters is most easily performed through CMS, this guide does not provide the command-line interface (CLI) procedures. For the cluster commands, refer to the *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference*.
- CLI command information—This guide provides an overview for using the CLI. For complete syntax and usage information about the commands that have been specifically created or changed for the Catalyst 2900 XL or Catalyst 3500 XL switches, refer to the *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference*.

Note This reference manual provides commands and command descriptions that have been created or changed for the Catalyst 2900 XL and Catalyst 3500 XL switches. It does not repeat the commands and command descriptions already documented in the Cisco IOS Release 12.0 documentation on Cisco.com.

Organization

The organization of this guide is as follows:

Chapter 1, "Overview," lists the software features of this release and provides examples of how the switch can be deployed in a network.

Chapter 2, "Getting Started with CMS," describes the Cluster Management Suite (CMS) web-based, switch management interface. Refer to the release notes for the procedures for configuring your web browser and accessing CMS. Refer to the online help for field-level descriptions of all CMS windows and procedures for using the CMS windows.

Chapter 3, "Getting Started with the CLI," describes the basics for using the Cisco IOS CLI.

Chapter 4, "General Switch Administration," includes the switch-configuration default settings and information about software releases, accessing the management interfaces, and using Simple Network Management Protocol (SNMP).

Chapter 5, "Clustering Switches," describes switch clusters and the considerations for creating and maintaining them. The online help provides the CMS procedures for configuring switch clusters. Cluster commands are described in the *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference*.

Chapter 6, "Configuring the System," provides the considerations and CLI procedures for configuring switch-wide settings. The online help provides the CMS procedures for configuring switch-wide settings.

Chapter 7, "Configuring the Switch Ports," provides the considerations and CLI procedures for configuring the switch ports. The online help provides the CMS procedures for configuring the switch ports.

Chapter 8, "Configuring VLANs," provides the considerations and CLI procedures for configuring VLANs. The online help provides the CMS procedures for configuring VLANs.

Chapter 9, "Troubleshooting," provides information about avoiding and resolving problems that might arise when you configure and maintain the switch.

Appendix A, "System Messages," lists the IOS system error messages for the switch.

Conventions

This guide uses these conventions to convey instructions and information:

Command descriptions use these conventions:

- Commands and keywords are in **boldface** text.
- Arguments for which you supply values are in *italic*.
- Square brackets ([ ]) indicate optional elements.
- Braces ({ }) group required choices, and vertical bars (|) separate the alternative elements.
- Braces and vertical bars within square brackets ([{ | }]) indicate a required choice within an optional element.

Interactive examples use these conventions:

- Terminal sessions and system displays are in `screen` font.
- Information you enter is in **`boldface screen`** font.
- Nonprinting characters, such as passwords or tabs, are in angle brackets (< >).

Notes, cautions, and tips use these conventions and symbols:

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Tip Means *the following will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information.

Related Publications

These documents provide complete information about the switch and are available from this Cisco.com site:

http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm

You can order printed copies of documents with a DOC-xxxxxx= number from the Cisco.com sites and from the telephone numbers listed in the "Ordering Documentation" section on page xvii.

- *Release Notes for the Catalyst 2900 Series XL and Catalyst 3500 Series XL Switches* (not orderable but is available on Cisco.com)

Note Switch requirements and procedures for initial configurations and software upgrades tend to change and therefore appear only in the release notes. Before installing, configuring, or upgrading the switch, refer to the release notes on Cisco.com for the latest information.

- *Catalyst 2900 Series XL and Catalyst 3500 Series XL Software Configuration Guide* (order number DOC-786511=)
- *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference* (order number DOC-7812155=)
- Cluster Management Suite (CMS) online help (available only from the switch CMS software)
- *Catalyst 2900 Series XL Hardware Installation Guide* (order number DOC-786461=)
- *Catalyst 3500 Series XL Hardware Installation Guide* (order number DOC-786456=)
- *Catalyst 2900 Series XL Modules Installation Guide* (order number DOC-CAT2900-IG=)
- *Catalyst 2900 Series XL ATM Modules Installation and Configuration Guide* (order number DOC-785472=)
- *1000BASE-T Gigabit Interface Converter Installation Note* (not orderable but is available on Cisco.com)
- *Catalyst GigaStack Gigabit Interface Converter Hardware Installation Guide* (order number DOC-786460=)

Obtaining Documentation

These sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at these sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

Cisco Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Cisco Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Registered Cisco Direct Customers

If you are a registered Cisco.com user (Cisco direct customer), you can order documentation as follows:

- Printed copies of Cisco product documentation are available from the Networking Products MarketPlace at this URL:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Part numbers for spare documentation are available from your local account representative or by selecting the documentation product family after choosing a Price List at:

  http://www.cisco.com/cgi-bin/order/pricing_root.pl?service=ViewByFamily1

- The Documentation CD (product number DOC-CONDOCCD=) is available from the Networking Products MarketPlace at this URL:

  http://www.cisco.com/cgi-bin/order/order_root.pl

Non-Registered Cisco.com Users

- If you are not a registered Cisco.com user, you can order printed copies of Cisco product documentation through a local account representative by calling Cisco Worldwide Sales at 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can send us your comments by completing the online survey. When you display the document listing for this platform, click **Give Us Your Feedback**. If you are using the product-specific CD and you are connected to the Internet, click the pencil-and-paper icon in the toolbar to display the survey. After you display the survey, select the manual that you wish to comment on. Click **Submit** to send your comments to the Cisco documentation group.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to this address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to this website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to this website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at this website:

http://www.cisco.com/tac/caseopen

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to this website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

Overview

This chapter provides these topics about the Catalyst 2900 XL and Catalyst 3500 XL switch software:

- Features, page 1-1
- Management Options, page 1-5
- Network Configuration Examples, page 1-7

Features

Note This guide describes the features for the Catalyst 2900 XL and Catalyst 3500 XL switches that are *not* Long-Reach Ethernet (LRE) switches. The Cisco IOS Release 12.0(5)WC3 software is for non-LRE switches only. Do not install this release on the Catalyst 2900 LRE XL switches. For configuring the Catalyst 2900 LRE XL switches, refer to Cisco IOS Release 12.0(5)WC2.

The Cisco IOS Release 12.0(5)WC3 software supports the hardware listed in the release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm).

Table 1-1 describes the features for this release. (Table 4-2 on page 4-8 lists the defaults for these features and includes references to where you can find additional information about each feature.)

Table 1-1 Features

Ease of Use and Ease of Deployment
• Cluster Management Suite (CMS) software for simplified switch and switch cluster management through a web browser, such as Netscape Communicator or Microsoft Internet Explorer, from anywhere in your intranet • Switch clustering technology, in conjunction with CMS, for – Unified configuration, monitoring, authentication, and software upgrade of multiple switches. Refer to the release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm) for a list of eligible cluster members. – Automatic discovery of candidate switches and creation of clusters of up to 16 switches that can be managed through a single IP address. – Extended discovery of cluster candidates that are not directly connected to the command switch. • Hot Standby Router Protocol (HSRP) for command-switch redundancy **Note** See the "Advantages of Using CMS and Clustering Switches" section on page 1-6. Refer to the release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm) for the CMS and cluster hardware, software, and browser requirements.
Performance
• Autosensing of speed on the 10/100 ports and autonegotiation of duplex mode on all switch ports for optimizing bandwidth • IEEE 802.3x flow control on the Gigabit ports operating in full-duplex mode • Fast EtherChannel and Gigabit EtherChannel for enhanced fault tolerance and for aggregating up to 8 ports of bandwidth between switches, routers, and servers • Per-port broadcast storm control for preventing faulty end stations from degrading overall system performance with broadcast storms • Cisco Group Management Protocol (CGMP) for limiting multicast traffic to specified end stations and reducing overall network traffic • CGMP Fast Leave for accelerating the removal of unused CGMP groups to reduce superfluous traffic on the network • Multicast VLAN registration (MVR) to continuously send multicast streams in a multicast VLAN, but to isolate the streams from subscriber VLANs for bandwidth and security reasons • Internet Group Management Protocol (IGMP) filtering for restricting the IP multicast groups that hosts connected to one or more switch ports can join • Protected port (private VLAN edge port) option for restricting the forwarding of traffic to designated ports on the same switch

Table 1-1 Features (continued)

Manageability
• Dynamic Host Configuration Protocol (DHCP)-based autoconfiguration for automatically configuring the switch during startup with IP address information and a configuration file that it receives during DHCP-based autoconfiguration **Note** DHCP replaces the Bootstrap Protocol (BOOTP) feature autoconfiguration to ensure retrieval of configuration files by unicast TFTP messages. BOOTP is available in earlier software releases for this switch. • Directed unicast requests to a Domain Name System (DNS) server for identifying a switch through its IP address and its corresponding host name • Address Resolution Protocol (ARP) for identifying a switch through its IP address and its corresponding Media Access Control (MAC) address • Cisco Discovery Protocol (CDP) versions 1 and 2 for network topology discovery and mapping between the switch and other Cisco devices on the network • Network Time Protocol (NTP) for providing a consistent timestamp to all switches from an external source • Directed unicast requests to a Trivial File Transfer Protocol (TFTP) server for administering software upgrades from a TFTP server • Default configuration stored in Flash memory to ensure that the switch can be connected to a network and can forward traffic with minimal user intervention • In-band management access through a CMS web-based session • In-band management access through up to 16 simultaneous Telnet connections for multiple command-line interface (CLI)-based sessions over the network • In-band management access through Simple Network Management Protocol (SNMP) versions 1 and 2c get and set requests • Out-of-band management access through the switch console port to a directly-attached terminal or to a remote terminal through a serial connection and a modem **Note** For additional descriptions of the management interfaces, see the "Management Options" section on page 1-5.
Redundancy
• HSRP for command switch redundancy • UniDirectional link detection (UDLD) on all Ethernet ports for detecting and disabling unidirectional links on fiber-optic interfaces caused by incorrect fiber-optic wiring or port faults • IEEE 802.1d Spanning Tree Protocol (STP) for redundant backbone connections and loop-free networks. STP has these features – Per-VLAN Spanning Tree (PVST) for balancing load across virtual LANs (VLANs) – Port Fast mode for eliminating forward delay by enabling a port to immediately change from a blocking state to a forwarding state – UplinkFast, Cross-Stack UplinkFast, and BackboneFast for fast convergence after a spanning-tree topology change and for achieving load balancing between redundant uplinks, including Gigabit uplinks and cross-stack Gigabit uplinks – STP root guard for preventing switches outside the core of the network from becoming the STP root **Note** Up to 64 instances of STP is supported on each switch (see Table 8-1 on page 8-2).

Table 1-1 Features (continued)

VLAN Support
• Depending on the switch model, up to 64 or 250 port-based VLANs are supported for assigning users to VLANs associated with appropriate network resources, traffic patterns, and bandwidth
Note For information about the maximum number of VLANs supported on each Catalyst 2900 XL and Catalyst 3500 XL switch, see the Table 8-1 on page 8-2.
• Inter-Switch Link (ISL) and IEEE 802.1Q trunking encapsulation on all ports for network moves, adds, and changes; management and control of broadcast and multicast traffic; and network security by establishing VLAN groups for high-security users and network resources
• VLAN Membership Policy Server (VMPS) for dynamic VLAN membership
• VLAN Trunking Protocol (VTP) pruning for reducing network traffic by restricting flooded traffic to links destined for stations receiving the traffic
Quality of Service and Class of Service
• IEEE 802.1p class of service (CoS) with two priority queues on the 10/100 switch ports and eight priority queues on the Gigabit ports for prioritizing mission-critical and time-sensitive traffic from data, voice, and telephony applications
• Voice VLAN (VVID) for creating subnets for voice traffic from Cisco IP Phones
Security
• Password-protected access (read-only and read-write access) to management interfaces (CMS and CLI) for protection against unauthorized configuration changes
• Multilevel security for a choice of security level, notification, and resulting actions
• Static MAC addressing for ensuring security
• MAC-based port security for restricting the use of a switch port to a specific group of source addresses and preventing switch access from unauthorized stations
• Terminal Access Controller Access Control System Plus (TACACS+), a proprietary feature for managing network security through a TACACS server
Monitoring
• Switch LEDs that provide visual management of port- and switch-level status
• MAC address notification for tracking the MAC addresses that the switch has learned or removed
• Switch Port Analyzer (SPAN) for complete traffic monitoring on any port
• Four groups (history, statistics, alarm, and events) of embedded remote monitoring (RMON) agents for network monitoring and traffic analysis
• Syslog facility for logging system messages about authentication or authorization errors, resource issues, and time-out events
Catalyst 3524-PWR XL Switch-Specific Support
• Ability to provide inline power to Cisco IP Phones from all 24 10/100 Ethernet ports
• Autodetection and control of inline phone power on a per-port basis on all 10/100 ports
• Fan-fault and over-temperature detection through Visual Switch Manager (VSM)

Management Options

The Catalyst 2900 XL and Catalyst 3500 XL switches are designed for plug-and-play operation: you only need to assign basic IP information to the switch and connect it to the other devices in your network. If you have specific network needs, you can configure and monitor the switch—on an individual basis or as part of a switch cluster—through its various management interfaces.

This section discusses these topics:

- Interface options for managing the switches
- Advantages of clustering switches and using CMS

Management Interface Options

You can configure and monitor individual switches and switch clusters by using these interfaces:

- CMS—CMS is a graphical user interface that can be launched from anywhere in your network through a web browser such as Netscape Communicator or Microsoft Internet Explorer. CMS is already installed on the switch. Using CMS, you can fully configure and monitor a standalone switch, a specific cluster member, or an entire switch cluster. You can also display network topologies to gather link information and to display switch images to modify switch- and port-level settings.

  For more information about CMS, see Chapter 2, “Getting Started with CMS.”

- CLI—The switch IOS CLI software is enhanced to support desktop-switching features. You can fully configure and monitor the switch and switch cluster members from the CLI. You can access the CLI either by connecting your management station directly to the switch console port or by using Telnet from a remote management station.

  For more information about the CLI, see Chapter 3, “Getting Started with the CLI.”

- SNMP—SNMP provides a means to monitor and control the switch and switch cluster members. You can manage switch configuration settings, performance, security, and collect statistics by using SNMP management applications such as CiscoWorks2000 LAN Management Suite (LMS) and HP OpenView.

  You can manage the switch from an SNMP-compatible management station that is running platforms such as HP OpenView or SunNet Manager. The switch supports a comprehensive set of MIB extensions and four RMON groups.

  For more information about using SNMP, see the “SNMP Network Management Platforms” section on page 4-5.

Advantages of Using CMS and Clustering Switches

Using CMS and switch clusters can simplify and minimize your configuration and monitoring tasks. You can use Cisco switch clustering technology to manage up to 16 interconnected supported Catalyst switches through one IP address as if they were a single entity. This can conserve IP addresses if you have a limited number of them. CMS is the easiest interface to use and makes switch and switch cluster management accessible to authorized users from any PC on your network.

By using switch clusters and CMS, you can

- Manage and monitor interconnected Catalyst switches, regardless of their geographic proximity and interconnection media, including Ethernet, Fast Ethernet, Fast EtherChannel, Cisco GigaStack Gigabit Interface Converter (GBIC), Gigabit Ethernet, and Gigabit EtherChannel connections. Refer to the release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm) for a list of supported switches.
- Accomplish multiple configuration tasks from a single CMS window without needing to remember CLI commands to accomplish specific tasks.
- Apply actions from CMS to multiple ports and multiple switches at the same time to avoid re-entering the same commands for each individual port or switch. Here are some examples of globally setting and managing multiple ports and switches:
  - Port configuration such as speed and duplex settings
  - Port and console port security
  - NTP, STP, VLAN, and quality of service (QoS) configuration
  - Inventory and statistic reporting and link- and switch-level monitoring and troubleshooting
  - Group software upgrade
- View a topology of interconnected devices to identify existing switch clusters and eligible switches that can join a cluster. You can also use the topology to quickly identify link information between switches.
- Monitor real-time status of a switch or multiple switches from the LEDs on the front-panel images. The system, redundant power system (RPS), and port LED colors on the images are similar to those used on the physical LEDs themselves.
- Use an interactive mode that takes you step-by-step through VLAN and voice VLAN (VVID) configuration
- Use a wizard that prompts you to provide only minimal required information to configure VVIDs

For more information about CMS, see Chapter 2, “Getting Started with CMS.” For more information about switch clusters, see Chapter 5, “Clustering Switches.”

Network Configuration Examples

This section provides network configuration concepts and includes examples of using the switch to create dedicated network segments and interconnecting the segments through Fast Ethernet and Gigabit Ethernet connections.

Design Concepts for Using the Switch

As your network users compete for network bandwidth, it takes longer to send and receive data. When you configure your network, consider the bandwidth required by your network users and the relative priority of the network applications they use.

Table 1-2 describes what can cause network performance to degrade and describes how you can configure your network to increase the bandwidth available to your network users.

Table 1-2 Increasing Network Performance

Network Demands	Suggested Design Methods
Too many users on a single network segment and a growing number of users accessing the Internet	• Create smaller network segments so that fewer users share the bandwidth, and use VLANs and IP subnets to place the network resources in the same logical network as the users who access those resources most. • Use full-duplex operation between the switch and its connected workstations.
• Increased power of new PCs, workstations, and servers • High demand from networked applications (such as e-mail with large attached files) and from bandwidth-intensive applications (such as multimedia)	• Connect global resources—such as servers and routers to which network users require equal access—directly to the Fast Ethernet or Gigabit Ethernet switch ports so that they have their own Fast Ethernet or Gigabit Ethernet segment. • Use the Fast EtherChannel or Gigabit EtherChannel feature between the switch and its connected servers and routers.

Bandwidth alone is not the only consideration when designing your network. As your network traffic profiles evolve, consider providing network services that can support applications such as voice and data integration and security.

Table 1-3 describes some network demands and how you can meet those demands.

Table 1-3 Providing Network Services

Network Demands	Suggested Design Methods
High demand for multimedia support	• Use CGMP and MVR to efficiently forward multicast traffic.
High demand for protecting mission-critical applications	• Use VLANs and protected ports to provide security and port isolation. • Use VLAN trunks, Cross-Stack UplinkFast, and BackboneFast for traffic-load balancing on the uplink ports so that the uplink port with a lower relative port cost is selected to carry the VLAN traffic.
An evolving demand for IP telephony	• Use QoS to prioritize applications such as IP telephony during congestion and to help control both delay and jitter within the network. • Use switches that support at least two queues per port to prioritize voice and data traffic as either high- or low-priority, based on 802.1p/Q. • Use VVIDs to provide a separate VLAN for voice traffic.
A growing demand for using existing infrastructure to transport data and voice from a home or office to the Internet or an intranet at higher speeds	• Use the Catalyst 2900 LRE XL switches to provide up to 15 Mb of IP connectivity over existing infrastructure (existing telephone lines). **Note** For more information about the Catalyst 2900 LRE XL switches and LRE technology, refer to the Catalyst 2900 XL and Catalyst 3500 XL documentation set for Cisco IOS Release 12.0(5.x)WC1 and Cisco IOS Release 12.0(5.x)WC2.

Figure 1-1 shows three configuration examples for using the Catalyst 2900 XL and Catalyst 3500 XL switches to create the following:

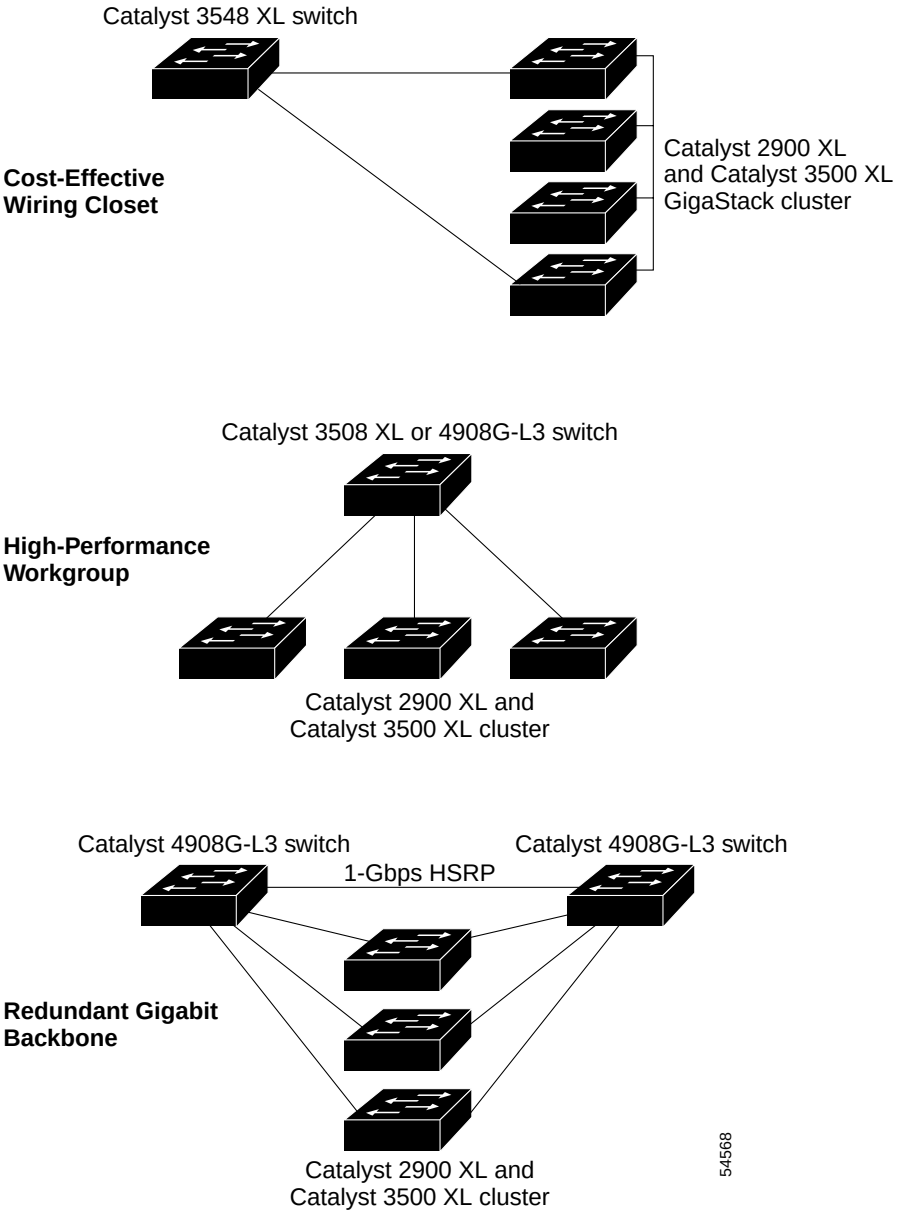
- Cost-effective wiring closet—A cost-effective way to connect many users to the wiring closet is to connect up to nine Catalyst 2900 and Catalyst 3500 XL switches through GigaStack GBIC connections. When you use a stack of Catalyst 3548 XL switches, you can connect up to 432 users. To preserve switch connectivity if one switch in the stack fails, connect the bottom switch to the top switch to create a GigaStack loopback and enable Cross-Stack UplinkFast on the cross-stack Gigabit uplinks.

  You can create backup paths by using Fast Ethernet, Gigabit, or Fast EtherChannel, or Gigabit EtherChannel links. Using Gigabit modules on two of the switches, you can have redundant uplink connections to a Gigabit backbone switch such as the Catalyst 3508G XL switch. If one of the redundant connections fails, the other can serve as a backup path. You can configure the stack members and the Catalyst 3508G XL switch as a switch cluster to manage them through a single IP address.

- High-performance workgroup—For users who require high-speed access to network resources, use Gigabit modules to connect the switches directly to a backbone switch in a star configuration. Each switch in this configuration provides users a dedicated 1-Gbps connection to network resources in the backbone. Compare this with the switches in a GigaStack configuration, where the 1-Gbps connection is shared among the switches. Using these Gigabit modules also provides flexibility in media and distance options:
  - 1000BASE-SX GBIC: fiber connections of up to 1804 ft (550 m)
  - 1000BASE-LX/LH GBIC: fiber connections of up to 32,808 ft (10 km)

  - 1000BASE-ZX GBIC: fiber connections of up to 328,084 ft (100 km)
  - 1000BASE-T GBIC: copper connections of up to 328 ft (100 m)
  - Catalyst 2900 XL 1000BASE-T: copper connections of up to 328 ft (100 m)
- Redundant Gigabit backbone—Using HSRP, you can create backup paths between Catalyst 4908G-L3 switches. To enhance network reliability and load balancing for different VLANs and subnets, you can connect the Catalyst 2900 XL and Catalyst 3500 XL switches, again in a star configuration, to two backbone switches. If one of the backbone switches fails, the second backbone switch preserves connectivity between the switches and network resources.

Figure 1-1 Example Configurations



Small to Medium-Sized Network Configuration

Figure 1-2 shows a configuration for a network that has up to 250 users. Users in this network require e-mail, file-sharing, database, and Internet access.

You optimize network performance by placing workstations on the same logical segment as the servers they access most often. This divides the network into smaller segments (or workgroups) and reduces the amount of traffic that travels over a network backbone, thereby increasing the bandwidth available to each user and improving server response time.

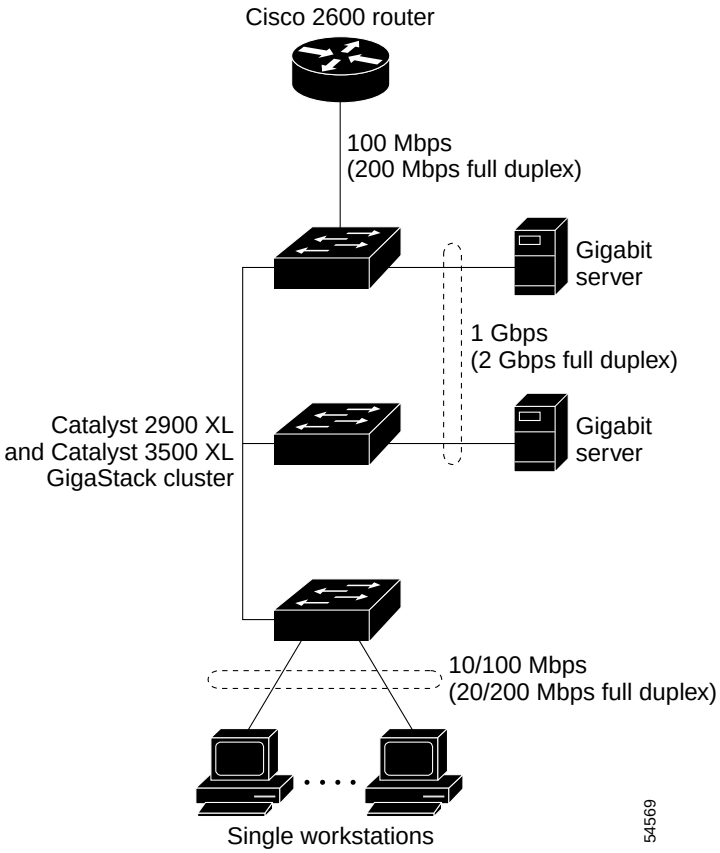
A *network backbone* is a high-bandwidth connection (such as Fast Ethernet or Gigabit Ethernet) that interconnects segments and network resources. It is required if numerous segments require access to the servers. The Catalyst 2900 XL and Catalyst 3500 XL switches in this network are connected through a GigaStack GBIC on each switch to form a 1-Gbps network backbone. This GigaStack can also be configured as a switch cluster, with primary and secondary command switches for redundant cluster management.

Workstations are connected directly to the 10/100 switch ports for their own 10- or 100-Mbps access to network resources (such as web and mail servers). When a workstation is configured for full-duplex operation, it receives up to 200 Mbps of dedicated bandwidth from the switch.

Servers are connected to the Gigabit module ports on the switches, allowing 1-Gbps throughput to users when needed. When the switch and server ports are configured for full-duplex operation, the links provide 2 Gbps of bandwidth. For networks that do not require Gigabit performance from a server, connect the server to a Fast Ethernet or Fast EtherChannel switch port.

Connecting a router to a Fast Ethernet switch port provides multiple, simultaneous access to the Internet through one line.

Figure 1-2 Small to Medium-Sized Network Configuration



Collapsed Backbone and Switch Cluster Configuration

Figure 1-3 shows a configuration for a network of approximately 500 employees. This network uses a collapsed backbone and switch clusters. A collapsed backbone has high-bandwidth uplinks from all segments and subnetworks to a single device, such as a Gigabit switch, which serves as a single point for monitoring and controlling the network. You can use a Catalyst 3550-12G switch, as shown, or a Catalyst 3508G XL switch to create a Gigabit backbone. A Catalyst 3550-12G backbone switch provides the benefits of inter-VLAN routing and allows the router to focus on WAN access.

The workgroups are created by clustering all the Catalyst switches. Using CMS and Cisco switch clustering technology, you can group the switches into multiple clusters, as shown, or into a single cluster. You can manage a cluster through the IP address of its active and standby command switches, regardless of the geographic location of the cluster members.

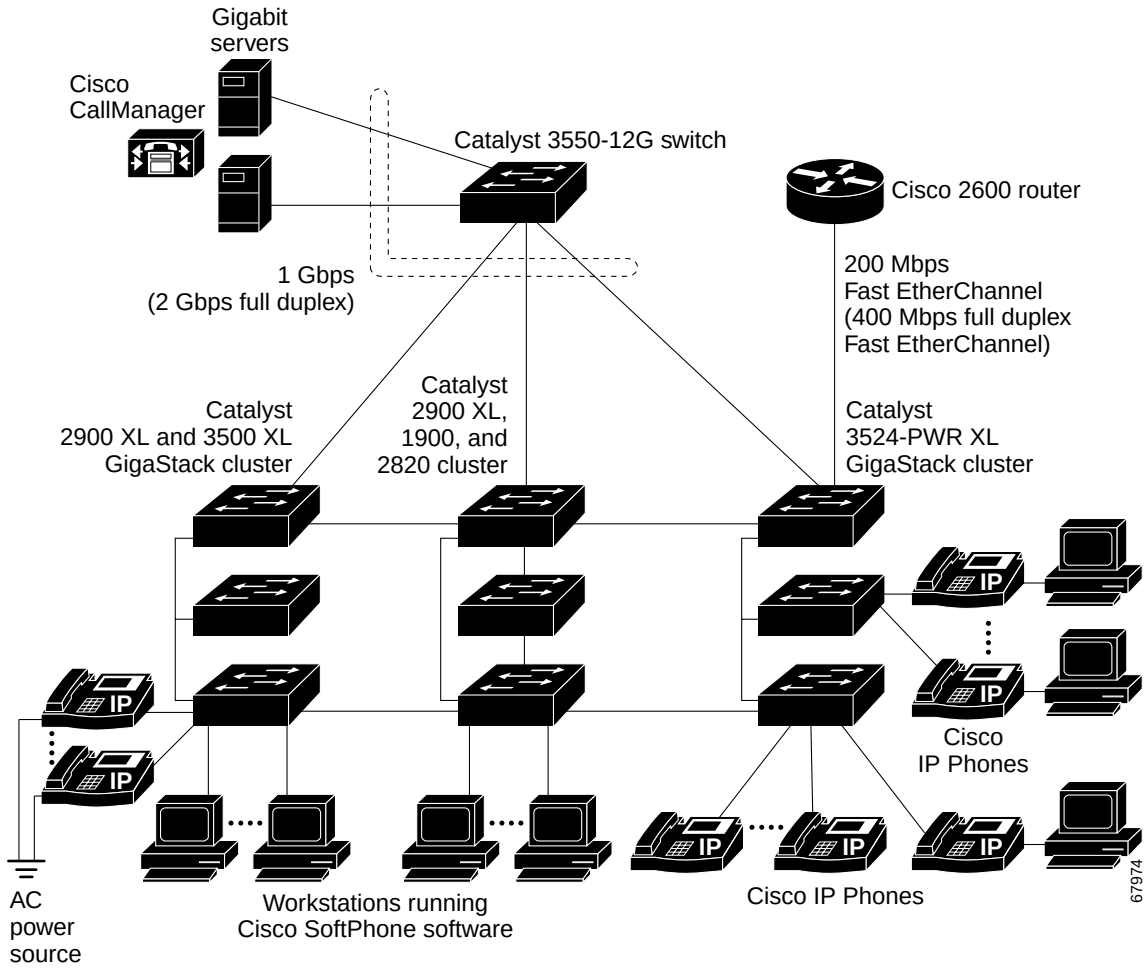
This network uses VLANs to segment the network logically into well-defined broadcast groups and for security management. Data and multimedia traffic are configured on the same VLAN. Voice traffic from the Cisco IP Phones are configured on separate VVIDs. For any switch port connected to Cisco IP Phones, 802.1p/Q QoS gives forwarding priority to voice traffic over data traffic.

Grouping servers in a centralized location provides benefits such as security and easier maintenance. The Gigabit connections to a server farm provide the workgroups full access to the network resources (such as a call-processing server running Cisco CallManager software, a DHCP server, or an IP/TV multicast server).

Cisco IP Phones are connected—using standard straight-through, twisted-pair cable with RJ-45 connectors—to the 10/100 inline-power ports on the Catalyst 3524-PWR XL switches and to the 10/100 ports on the Catalyst 2900 XL and Catalyst 3500 XL switches. These multiservice switch ports automatically detect if an IP phone is connected. Cisco CallManager controls call processing, routing, and IP phone features and configuration. Users with workstations running Cisco SoftPhone software can place, receive, and control calls from their PCs. Using Cisco IP Phones, Cisco CallManager software, and Cisco SoftPhone software integrates telephony and IP networks, where the IP network supports both voice and data.

Each 10/100 inline-power port on the Catalyst 3524-PWR XL switches provides –48 VDC power to the Cisco IP Phone. The IP phone can receive redundant power when it also is connected to an AC power source. IP phones not connected to the Catalyst 3524-PWR XL switches receive power from an AC power source.

Figure 1-3 Collapsed Backbone and Switch Cluster Configuration



Large Campus Configuration

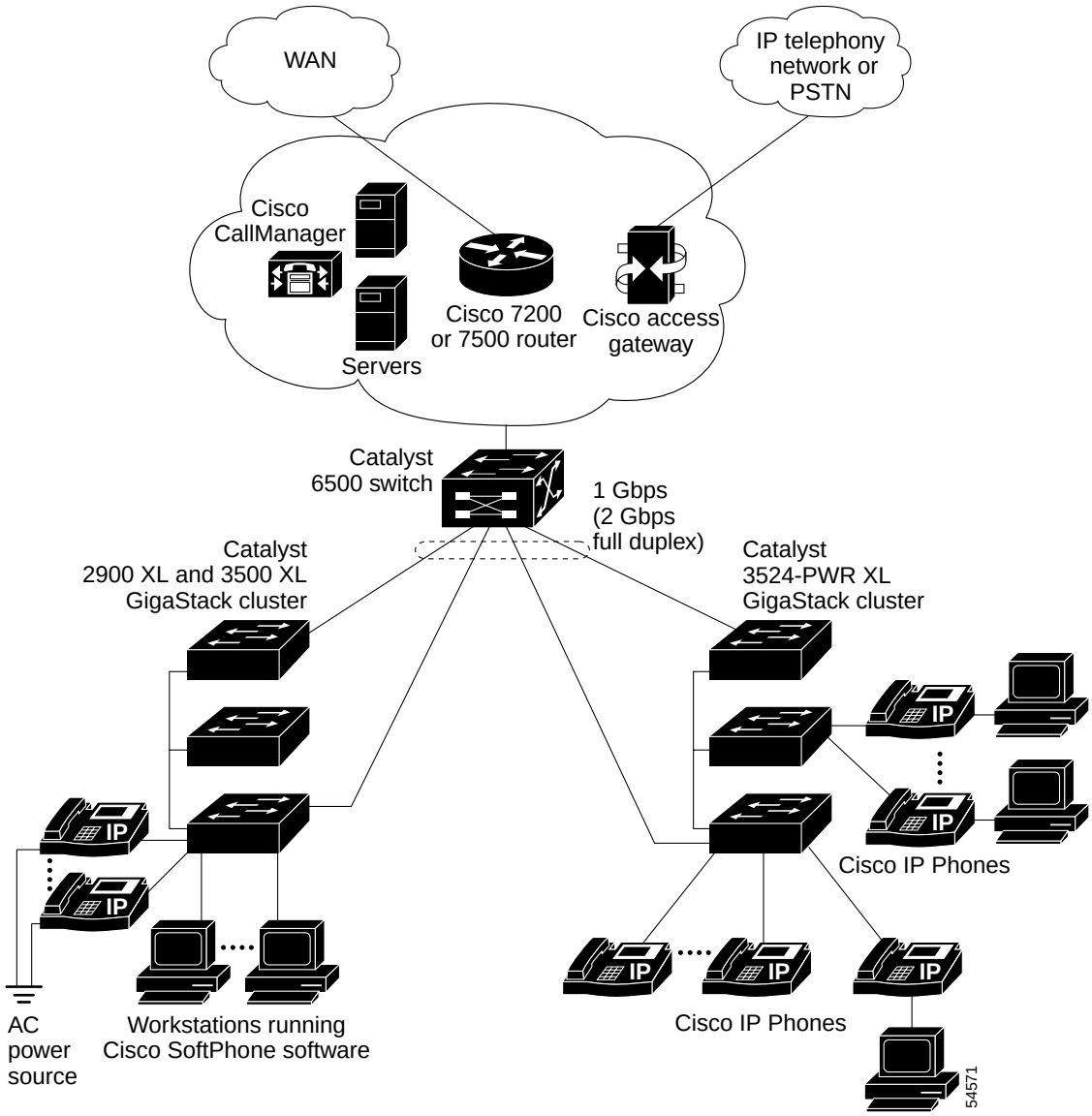
Figure 1-4 shows a configuration for a network of more than 1000 users. Because it can aggregate up to 130 Gigabit connections, a Catalyst 6500 multilayer switch is used as the backbone switch.

You can use the workgroup configurations shown in previous examples to create workgroups with Gigabit uplinks to the Catalyst 6500 switch. For example, you can use switch clusters that have a mix of Catalyst 2900 XL and Catalyst 3500 XL switches.

The Catalyst 6500 switch provides the workgroups with Gigabit access to core resources:

- Cisco 7000 series router for access to the WAN and the Internet.
- Server farm that includes a call-processing server running Cisco CallManager software. Cisco CallManager controls call processing, routing, and IP phone features and configuration.
- Cisco Access gateway (such as Cisco Access Digital Trunk Gateway or Cisco Access Analog Trunk Gateway) that connects the IP network to the PSTN or to users in an IP telephony network.

Figure 1-4 Large Campus Configuration



Multidwelling Configuration

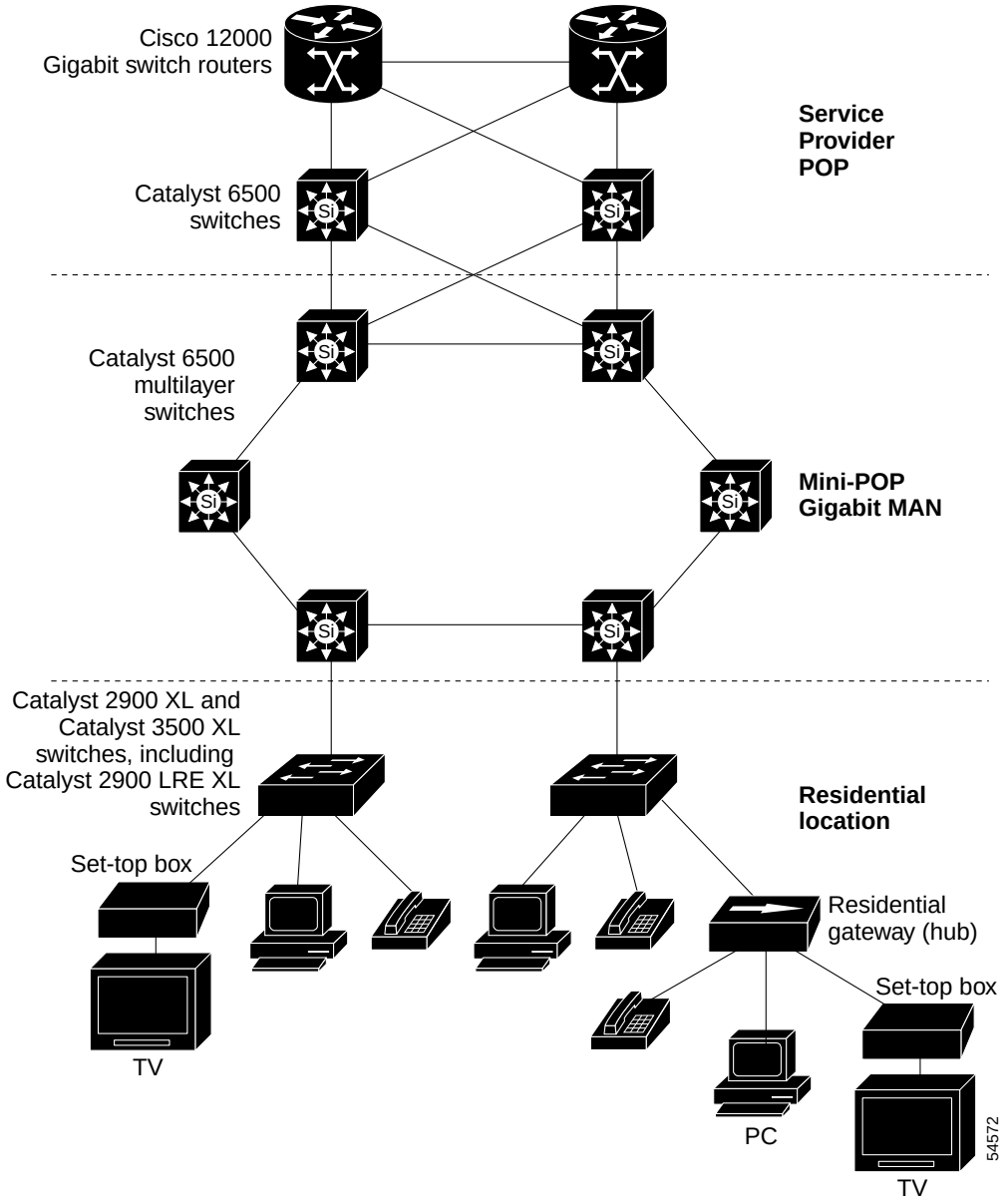
A growing segment of residential and commercial customers are requiring high-speed access to Ethernet metropolitan-area networks (MANs). Figure 1-5 shows a configuration for a Gigabit Ethernet MAN ring using Catalyst 6500 switches as aggregation switches in the mini-point-of-presence (POP) location. These switches are connected through 1000BASE-X GBIC ports.

The resident switches can be Catalyst 2900 XL and Catalyst 3500 XL switches, providing customers with either Fast Ethernet or Gigabit Ethernet connections to the MAN. Catalyst 2900 LRE XL switches can also be used as residential switches for customers requiring connectivity through existing telephone lines. The Catalyst 2900 LRE XL switches can then connect to another residential switch through a 10/100 connection.

For more information about the Catalyst 2900 LRE XL switches and LRE technology, refer to the Catalyst 2900 XL and Catalyst 3500 XL documentation set for Cisco IOS Release 12.0(5.x)WC1 and Cisco IOS Release 12.0(5.x)WC2.

All ports on the residential switches are configured as 802.1Q trunks with the protected port and STP root guard options enabled. The protected port option provides security and isolation between ports on the switch, ensuring that subscribers cannot view packets destined for other subscribers. STP root guard prevents unauthorized devices from becoming the STP root switch. All ports have CGMP enabled for multicast traffic management.

Figure 1-5 Multidwelling Configuration



Getting Started with CMS

This chapter provides these topics about the Cluster Management Suite (CMS) software:

- Features, page 2-2
- Front Panel View, page 2-4
- Topology View, page 2-13
- Menus and Toolbar, page 2-18
- Interaction Modes, page 2-28
- Wizards, page 2-28
- Online Help, page 2-29
- CMS Window Components, page 2-30
- Accessing CMS, page 2-32
- Verifying Your Changes, page 2-34
- Saving Your Changes, page 2-34
- Using Different Versions of CMS, page 2-35
- Where to Go Next, page 2-35

Note

- For system requirements and for browser and Java plug-in configuration procedures, refer to the release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm).
- For procedures for using CMS, refer to the online help.

Note This chapter describes the CMS interface of the Catalyst 2900 XL and Catalyst 3500 XL switches. Refer to the appropriate switch documentation for descriptions of the web-based management software used on other Catalyst switches.

Features

CMS provides these features (Figure 2-1) for managing switch clusters and individual switches from Web browsers such as Netscape Communicator or Microsoft Internet Explorer:

- Two views of your network that can be displayed at the same time:
  - The Front Panel view displays the front-panel image of a specific switch or the front-panel images of all switches in a cluster. From this view, you can select multiple ports or multiple switches and configure them with the same settings.

    When CMS is launched from a command switch, the Front Panel view displays the front-panel images of all switches in the cluster. When CMS is launched from a noncommand switch, the Front Panel view displays only the front panel of the specific switch.

Note CMS from a standalone switch or from a noncommand switch is referred to as *Device Manager* (also referred to as *Switch Manager*). Device Manager is for configuring an individual switch. When you select Device Manager for a specific switch in the cluster, you launch a separate CMS session. The Device Manager interface can vary between the Catalyst switch platforms.

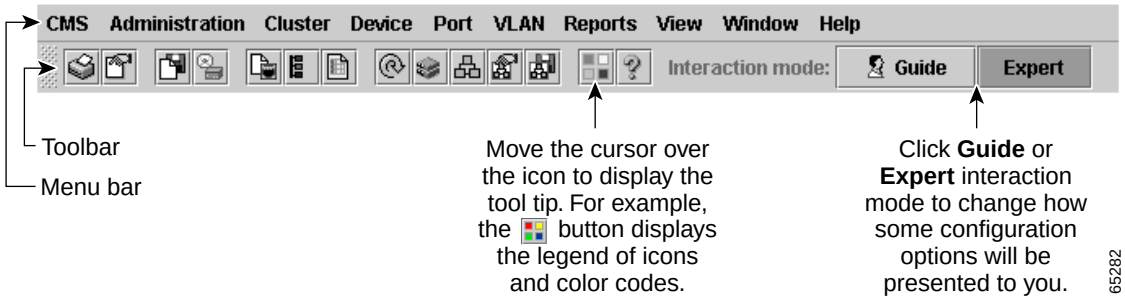
  - The Topology view displays a network map that uses icons that represent switch clusters, cluster members, cluster candidates, neighboring devices that are not eligible to join a cluster, and link types. From this view, you can select multiple switches and configure them to run with the same settings. You can also display link information in the form of link reports and link graphs.

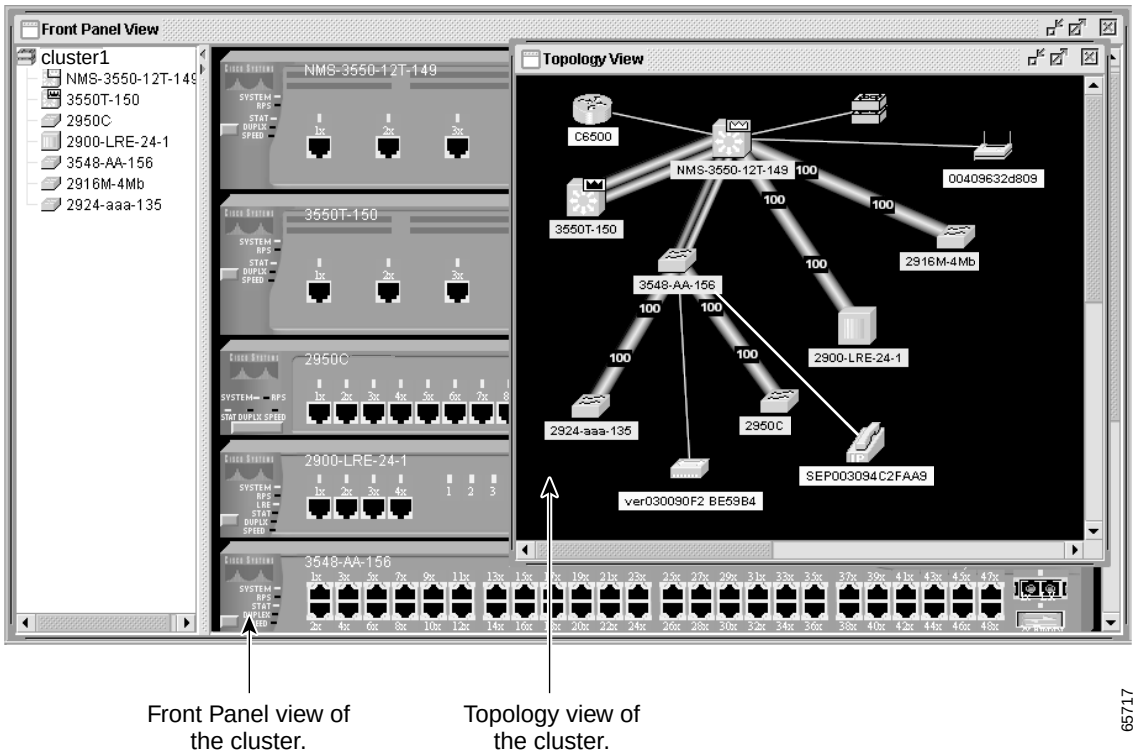
    This view is available only when CMS is launched from a command switch.
- Menus and toolbar to access configuration and management options:
  - The menu bar provides the complete list of options for managing a single switch and switch clusters.
  - The toolbar provides buttons for commonly used switch and cluster configuration options and information windows such as legends and online help.
  - The port popup menu, in the Front Panel view, provides options specific for configuring and monitoring switch ports.
  - The device popup menu, in either the Front Panel or the Topology views, provides switch and cluster configuration and monitoring options.
  - The candidate, member, and link popup menus provide options for configuring and monitoring devices and links in the Topology view.

  The toolbar and popup menus provide quick ways to access frequently used menu-bar options.
- Tools to simplify configuration tasks:
  - Interactive modes—guide mode and expert mode—that control the presentation of some complex configuration options
  - Wizards that require minimal information from you to configure some complex features
  - Comprehensive online help that provides high-level concepts and procedures for performing tasks from the window

- Two levels of access to the configuration options: read-write access for users allowed to change switch settings; read-only access for users allowed to only view switch settings
- Consistent set of GUI components (such as tabs, buttons, drop-down lists, tables, and so on) for a consistent approach to setting configuration parameters

Figure 2-1 CMS Features





Front Panel View

When CMS is launched from a command switch, the Front Panel view displays the front-panel images of all switches in the cluster (Figure 2-2). When CMS is launched from a standalone or non-command member switch, the Front Panel view displays only the front panel of the specific switch (Figure 2-3).

Figure 2-2 Front Panel View from a Standalone Switch

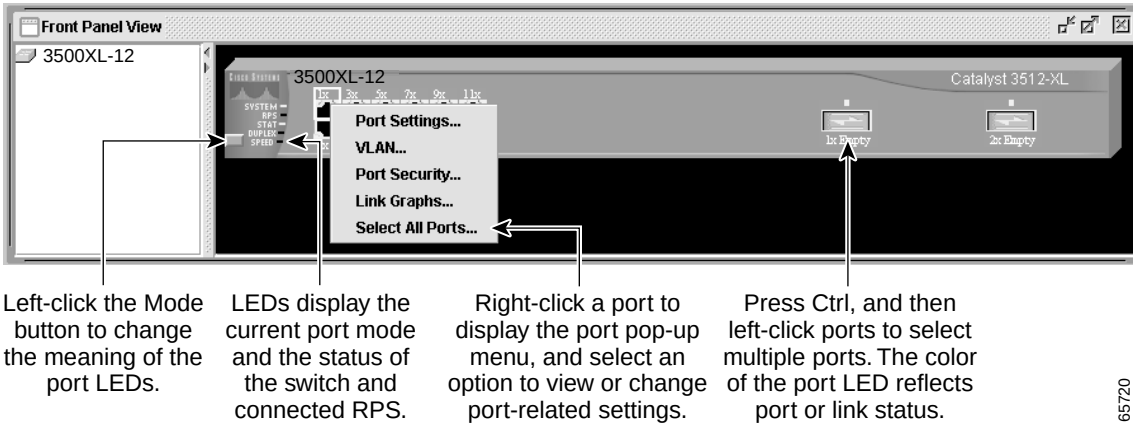
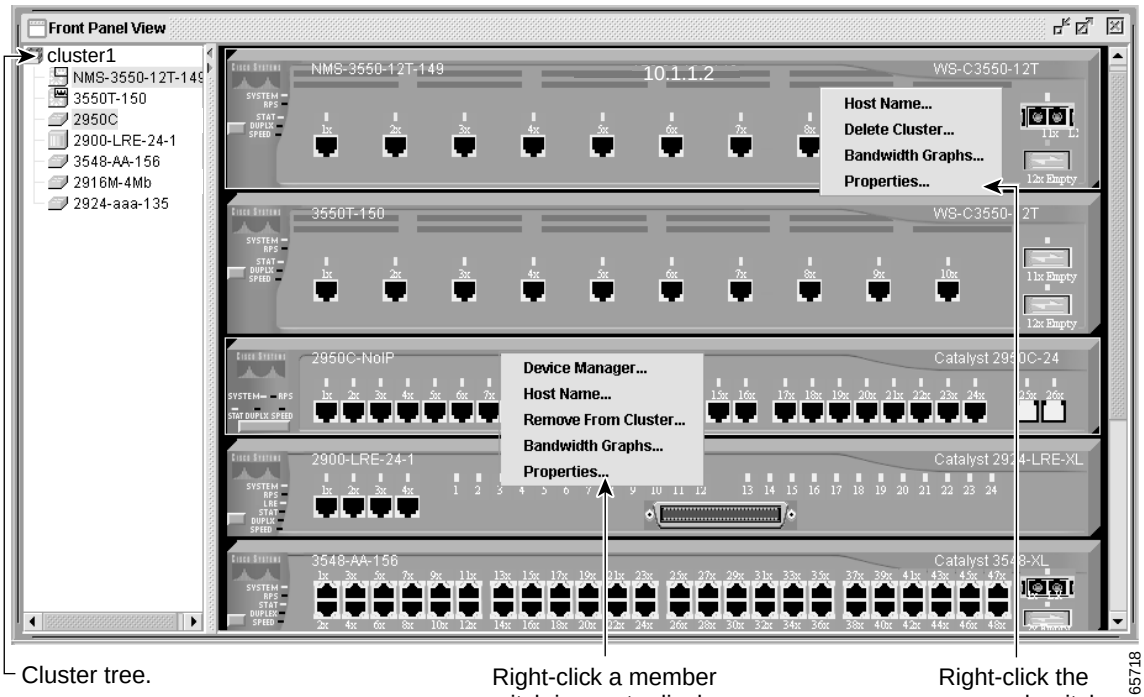

Front Panel View
3500XL-12
3500XL-12
Catalyst 3512-XL
Port Settings...
VLAN...
Port Security...
Link Graphs...
Select All Ports...
Left-click the Mode button to change the meaning of the port LEDs.
LEDs display the current port mode and the status of the switch and connected RPS.
Right-click a port to display the port pop-up menu, and select an option to view or change port-related settings.
Press Ctrl, and then left-click ports to select multiple ports. The color of the port LED reflects port or link status.
65720

Figure 2-3 Front Panel View from a Command Switch



Cluster Tree

The cluster tree (Figure 2-3) appears in the left frame of the Front Panel view and shows the name of the cluster and a list of its members. The sequence of the cluster-tree icons (Figure 2-4) mirror the sequence of the front-panel images. You can change the sequence by selecting **View > Arrange Front Panel**. The colors of the devices in the cluster tree reflect the status of the devices (Table 2-1).

If you want to configure switch or cluster settings on one or more switches, select the appropriate front-panel images.

- To select a front-panel image, click either the cluster-tree icon or the corresponding front-panel image. The front-panel image is then highlighted with a yellow outline.
- To select multiple front-panel images, press the **Ctrl** key, and left-click the cluster-tree icons or the front-panel images. To deselect an icon or image, press the **Ctrl** key, and left-click the icon or image.

If the cluster has many switches, you might need to scroll down the window to display the rest of front-panel images. Instead of scrolling, you can click an icon in the cluster tree, and CMS then scrolls and displays the corresponding front-panel image.

Figure 2-4 Cluster-Tree Icons

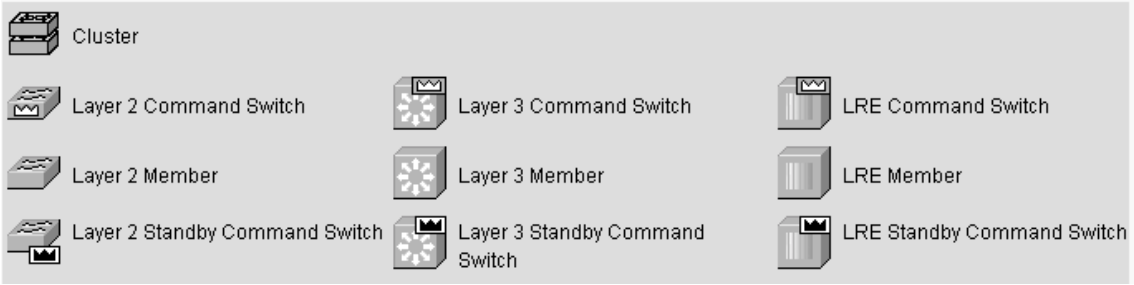


Table 2-1 Cluster Tree Icon Colors

Color	Device Status
Green	Switch is operating normally.
Yellow	The internal fan of the switch is not operating, or the switch is receiving power from an RPS.
Red	Switch is not powered up, has lost power, or the command switch is unable to communicate with the member switch.

Front-Panel Images

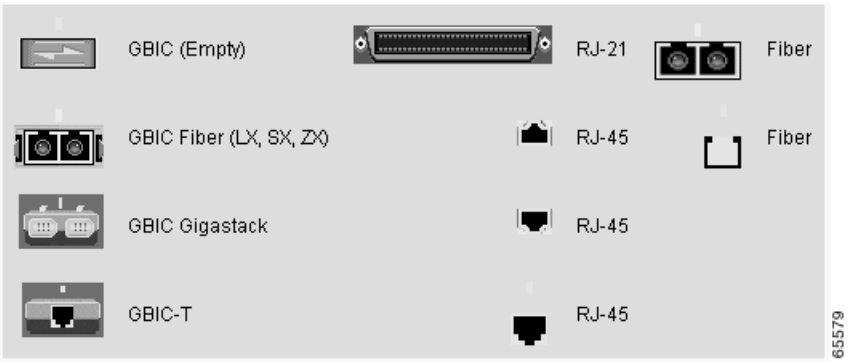
You can manage the switch from a remote station by using the front-panel images. The front-panel images are updated based on the network polling interval that you set from **CMS > Preferences**.

Note The Preferences window is not available if your switch access level is read-only. For more information about the read-only access mode, see the "Access Modes in CMS" section on page 2-33.

Figure 2-5 shows the port icons as they appear in the front-panel images. To select a port, click the port on the front-panel image. The port is then highlighted with a yellow outline. To select multiple ports, you can:

- Press the left mouse button, drag the pointer over the group of ports that you want to select, and then release the mouse button.
- Press the **Ctrl** key, and click the ports that you want to select.
- Right-click a port, and select **Select All Ports** from the port popup menu.

Figure 2-5 Port Icons



The following sections provide complete descriptions of the LED images. Similar descriptions of these LEDs are provided in the switch hardware installation guide.

Redundant Power System LED

The Redundant Power System (RPS) LED shows the RPS status (Table 2-2 and Table 2-3). Certain switches in the switch cluster use a specific RPS model:

- Cisco RPS 300 (model PWR300-AC-RPS-N1)—Catalyst 2900 LRE XL, Catalyst 2950, Catalyst 3524-PWR XL, and Catalyst 3550 switches
- Cisco RPS 600 (model PWR600-AC-RPS)—Catalyst 2900 XL and Catalyst 3500 XL switches, except the Catalyst 2900 LRE XL and Catalyst 3524-PWR XL switches

Refer to the appropriate switch hardware documentation for RPS descriptions specific for the switch.

Table 2-2 Cisco RPS 300 LED on the Catalyst 2900 LRE XL, Catalyst 2950, Catalyst 3524-PWR XL, and Catalyst 3550 Switches

Color	RPS Status
Black (off)	RPS is off or is not installed.
Green	RPS is connected and operational.
Blinking green	RPS is providing power to another switch in the stack.
Amber	RPS is connected but not functioning. The RPS could be in standby mode. To put the RPS in Active mode, press the Standby/Active button on the RPS, and the LED should turn green. If it does not, one of these conditions could exist: • One of the RPS power supplies could be down. Contact Cisco Systems. • The RPS fan could have failed. Contact Cisco Systems.
Blinking amber	Internal power supply of the switch is down, and redundancy is lost. The switch is operating on the RPS.

Table 2-3 Cisco RPS 600 LED on the Catalyst 2900 XL and Catalyst 3500 XL Switches Except the Catalyst 2900 LRE XL, and Catalyst 3524-PWR XL Switches

Color	RPS Status
Black (off)	RPS is off or is not installed.
Green	RPS is operational.
Blinking green	RPS and the switch AC power supply are both powered up. If the switch power supply fails, the switch powers down and after 15 seconds restarts, using power from the RPS. The switch goes through its normal boot sequence when it restarts. **Note** This is not a recommended configuration.
Amber	RPS is connected but not functioning properly. One of the power supplies in the RPS could be powered down, or a fan on the RPS could have failed.

Port Modes and LEDs

The port modes (Table 2-5) determine the type of information displayed through the port LEDs. When you change port modes, the meanings of the port LED colors (Table 2-6, Table 2-7, and Table 2-8) also change.

Note The bandwidth utilization mode (UTL LED) does not appear on the front-panel images. Select **Reports > Bandwidth Graphs** to display the total bandwidth in use by the switch. Refer to the switch hardware installation guide for information about using the UTL LED.

To select or change a mode, click the Mode button until the desired mode LED is green.

Table 2-5 Port Modes

Mode LED	Description
STAT	Ethernet link status of the 10/100, 100BASE-FX, or 1000BASE-X switch ports, or the Ethernet link status on the remote customer premises equipment (CPE). Default mode on all Catalyst 2900 XL and Catalyst 3500 XL switches except the Catalyst 2900 LRE XL switches.
LRE (Catalyst 2900 LRE XL only)	Long-Reach Ethernet (LRE) link status of the LRE ports on the Catalyst 2900 LRE XL switches. Default mode on these switches only. **Note** When the LRE mode is active, the 10/100 switch ports on the Catalyst 2900 LRE XL continue to show Ethernet link status.
FDUP or DUPLX	Duplex setting on the ports. • Default setting is auto on all Catalyst 2900 XL and Catalyst 3500 XL switches and on the 10/100 ports on the Catalyst 2900 LRE XL switches. • Default setting is half-duplex on the LRE ports on the Catalyst 2900 LRE XL switches. **Note** On the Catalyst 2900 LRE XL switches, this LED shows the duplex mode used on the Ethernet link between the remote CPE and Ethernet device.
SPEED or SPD	Speed setting on the ports. Default setting is auto. **Note** On the Catalyst 2900 LRE XL switches, this LED shows the link speed between the remote CPE and Ethernet device.
LINE PWR (Catalyst 3524-PWR XL only)	Inline power setting on the Catalyst 3524-PWR XL 10/100 ports. Default setting is auto.

Table 2-6 Port LEDs on the Catalyst 2912, 2924C, 2924, 2912MF, and 2924M XL Switches [1]

Port Mode	Port LED Color	Description
STAT	Cyan (off)	No link.
	Green	Link present.
	Blinking green	Activity on the port. Port is transmitting or receiving data.
	Amber	Link fault. Error frames can affect connectivity, and errors such as excessive collisions, CRC errors, and alignment and jabber errors are monitored for a link-fault indication. Port is not forwarding. Port was disabled by management, or by an address violation, or was blocked by Spanning Tree Protocol (STP). **Note** After a port is reconfigured, the port LED can remain amber for up to 30 seconds as STP checks the switch for possible loops.
	Brown	No link and port is administratively shut down.
FDUP	Cyan (off)	Port is operating in half-duplex mode.
	Green	Port is operating in full-duplex mode.
SPD	Cyan (off)	Port is operating at 10 Mbps.
	Green	Port is operating at 100 Mbps.

1. On the modular switches, port LED 1 or 2 is green when a module is installed. Refer to the module documentation for complete information.

Table 2-7 LRE Port LEDs on the Catalyst 2900 LRE XL Switches[1]

Port Mode	Port LED Color	Description
LRE[2]	Cyan (off)	No LRE link present on the LRE port.
	Green	LRE link present on the LRE port. Port LED turns green in approximately 10 seconds after the LRE port detects a connection to a Cisco 575 LRE CPE.
	Amber	LRE port on the switch and WALL port on the Cisco 575 LRE CPE unable to establish the rate defined by the assigned profile. Refer to the switch software guide for Cisco IOS Release 12.0(5)WC(1).
STAT	Cyan (off)	No Ethernet link present on the 10/100 switch port or on the remote CPE Ethernet port.
	Green	Ethernet link present on the 10/100 switch port or on the remote CPE Ethernet port.
	Blinking green	Activity on the 10/100 switch port or on the remote CPE Ethernet port. Port is transmitting or receiving data.
	Amber	Link fault. Error frames can affect connectivity, and errors such as excessive collisions, CRC errors, and alignment and jabber errors are monitored for a link-fault indication. 10/100 switch port or remote CPE Ethernet port is not forwarding. Port was disabled by management, by an address violation, or was blocked by STP. **Note** After a port is reconfigured, the port LED can remain amber for up to 30 seconds as STP checks the switch for possible loops.
	Brown	No link and port is administratively shut down.
DUPLX	Cyan (off)	10/100 switch port or remote CPE Ethernet port is operating in half-duplex mode.
	Green	10/100 switch port or remote CPE Ethernet port is operating in full-duplex mode.
SPEED	Cyan (off)	10/100 switch port or remote CPE Ethernet port is operating at 10 Mbps.
	Green	10/100 switch port or remote CPE Ethernet port is operating at 100 Mbps.

1. In STAT mode, the LRE ports reflect the Ethernet link between the remote CPE and Ethernet device such as a PC. The Ethernet link default settings on the LRE ports are different than those on the 10/100 ports. See Table 2-5.
2. In LRE mode, the 10/100 port LEDs continue to reflect Ethernet link status.

Table 2-8 Port LEDs on the Catalyst 3500 XL Switches

Port Mode	Port LED Color	Description
STATUS	Cyan (off)	No link.
	Green	Link present.
	Blinking green	Activity on the port. Port is transmitting or receiving data.
	Amber	Link fault. Error frames can affect connectivity, and errors such as excessive collisions, CRC errors, and alignment and jabber errors are monitored for a link-fault indication. Port is not forwarding. Port was disabled by management, by an address violation, or was blocked by STP. **Note** After a port is reconfigured, the port LED can remain amber for up to 30 seconds as STP checks the switch for possible loops.
	Brown	No link and port is administratively shut down.
DUPLEX	Cyan (off)	Port is operating in half-duplex mode.
	Green	Port is operating in full-duplex mode.
SPEED	**10/100 Ports**	
	Cyan (off)	Port is operating at 10 Mbps.
	Green	Port is operating at 100 Mbps.
	1000BASE-X Ports	
	Cyan (off)	Port is not operating.
	Green	Port is operating at 1000 Mbps.
LINE PWR (Catalyst 3524-PWR XL only)	Cyan (off)	Inline power is off.
	Green	Inline power is on. If the Cisco IP Phone is receiving power from an AC power source, the port LED is off even if the IP phone is connected to the switch port. The LED turns green only when the switch port is providing power.

VLAN Membership Modes

Ports in the Front Panel view are outlined by colors (Table 2-9) when you click **Highlight VLAN Port Membership Modes** on the Configure VLANs tab on the VLAN window (**VLAN > VLAN > Configure VLANs**). The colors show the VLAN membership mode of each port. The VLAN membership mode determines the kind of traffic the port carries and the number of VLANs it can belong to. For more information about these modes, see the "Assigning VLAN Port Membership Modes" section on page 8-5.

Note This feature is not supported on the Catalyst 1900 and Catalyst 2820 switches.

Table 2-9 VLAN Membership Modes

Mode	Color
Static access	Light green
Dynamic access	Pink
ISL trunk	Orange
Multi-VLAN	Yellow
802.1Q trunk	Peach
ATM trunk	Purple

Topology View

The Topology view displays how the devices within a switch cluster are connected and how the switch cluster is connected to other clusters and devices. From this view, you can add and remove cluster members. This view provides two levels of detail of the network topology:

- When you right-click a cluster icon and select Expand Cluster, the Topology view displays the switch cluster in detail. This view shows the command switch and member switches in a cluster. It also shows candidate switches that can join the cluster. This view does not display the details of any neighboring switch clusters (Figure 2-6).
- When you right-click a command-switch icon and select Collapse Cluster, the cluster is collapsed and represented by a single icon. The view shows how the cluster is connected to other clusters, candidate switches, and devices that are not eligible to join the cluster (such as routers, access points, IP phones, and so on) (Figure 2-7).

Note The Topology view displays only the switch cluster and network neighborhood of the specific command or member switch that you access. To display a different switch cluster, you need to access the command switch or member switch of that cluster.

You can arrange the device icons in this view. To move a device icon, click and drag the icon. To select multiple device icons, you can either:

- Press the left mouse button, drag the pointer over the group of device icons that you want to select, and then release the mouse button.
- Press the **Ctrl** key, and click the device icons that you want to select.

After selecting the icons, drag the icons to any area in the view.

Figure 2-6 Expand Cluster View

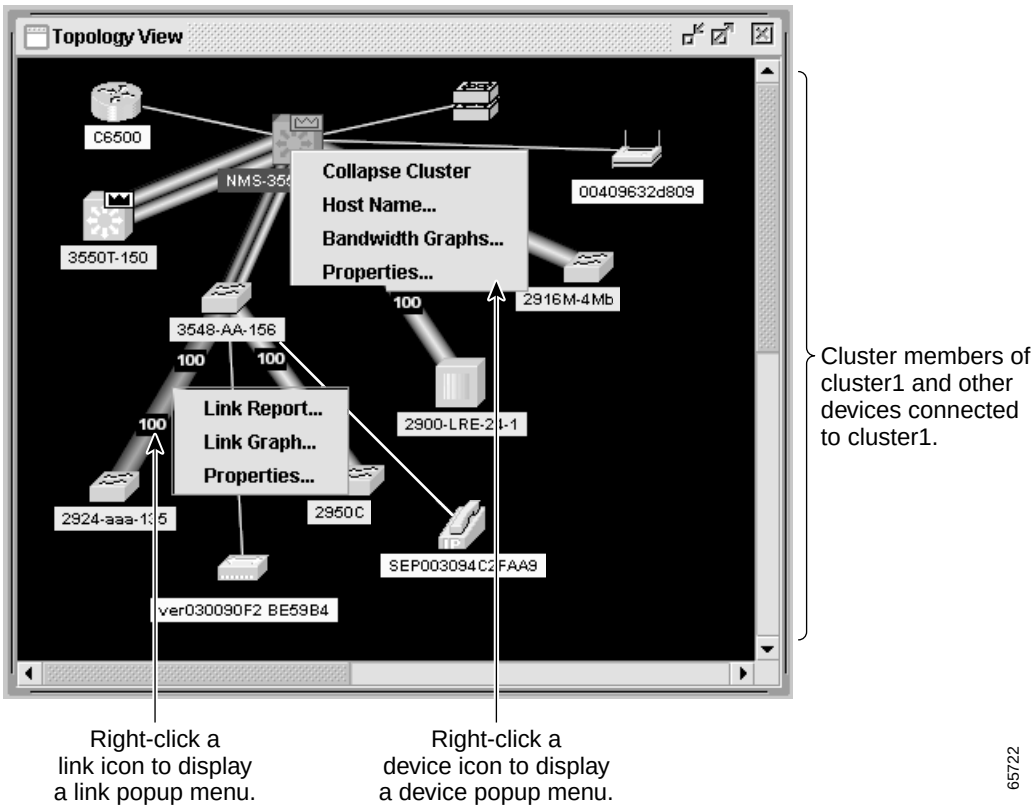
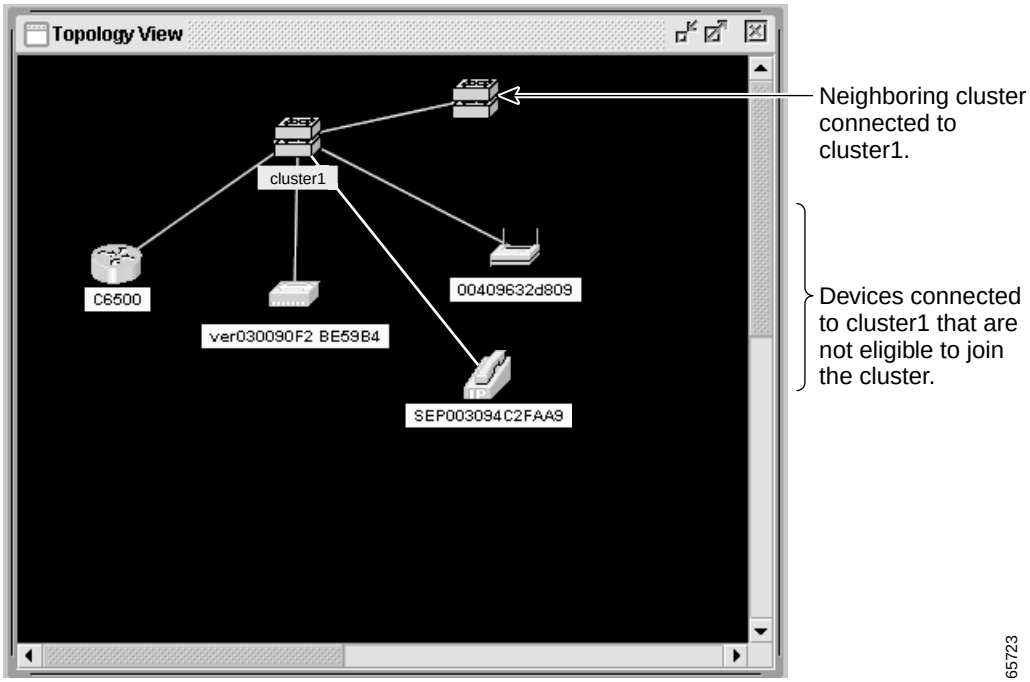


Figure 2-7 Collapse Cluster View



Topology Icons

The Topology view and the cluster tree use the same set of device icons to represent clusters, command and standby command switches, and member switches (Figure 2-8). The Topology view also uses additional icons to represent these types of neighboring devices:

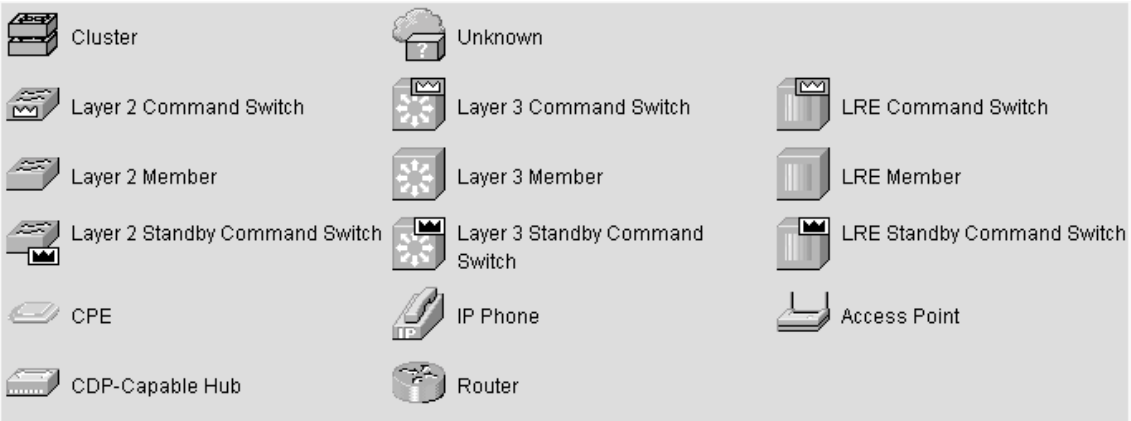
- Customer premises equipment (CPE) devices that are connected to Long-Reach Ethernet (LRE) switches
- Devices that are not eligible to join the cluster, such as Cisco IP phones, Cisco access points, and Cisco Discovery Protocol (CDP)-capable hubs and routers
- Devices that are identified as *unknown* devices, such as some Cisco devices and third-party devices

Note Candidate switches are distinguished by the color of their device label. Device labels and their colors are described in the "Colors in the Topology View" section on page 2-17.

To select a device, click the icon. The icon is then highlighted. To select multiple devices, you can either:

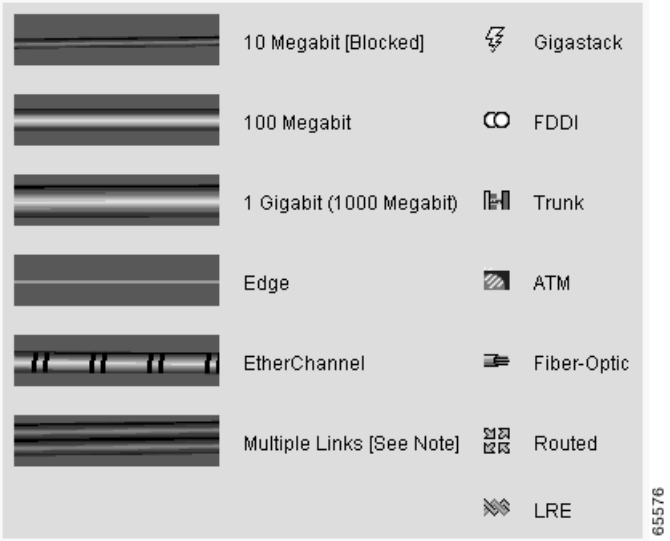
- Press the left mouse button, drag the pointer over the group of icons that you want to select, and then release the mouse button.
- Press the **Ctrl** key, and click the icons that you want to select.

Figure 2-8 Topology-View Device Icons



The Topology view also uses a set of link icons (Figure 2-9) to show the link type and status between two devices. To select a link, click the link that you want to select. To select multiple links, press the Ctrl key, and click the links that you want to select.

Figure 2-9 Topology-View Link Icons



Device and Link Labels

The Topology view displays device and link information by using these *labels*:

- Cluster and switch names
- Switch MAC and IP addresses
- Link type between the devices
- Link speed and IDs of the interfaces on both ends of the link

When using these labels, keep these considerations in mind:

- The IP address displays only in the labels for the command switch and member switches.
- The label of a neighboring cluster icon only displays the IP address of the command-switch IP address.
- The displayed link speeds are the actual link speeds except on the LRE links, which display the administratively assigned speed settings.

You can change the label settings from the Topology Options window, which is displayed by selecting **View > Topology Options**.

Colors in the Topology View

The colors of the Topology view icons reflect the status of the devices and links (Table 2-10, Table 2-11, and Table 2-12).

Table 2-10 Device Icon Colors

Icon Color	Color Meaning
Green	The device is operating.
Yellow[1]	The internal fan of the switch is not operating, or the switch is receiving power from an RPS.
Red[1]	The device is not operating.

1. Available only on the cluster members.

Table 2-11 Single Link Icon Colors

Link Color	Color Meaning
Green	Active link
Red	Down or blocked link

Table 2-12 Multiple Link Icon Colors

Link Color	Color Meaning
Both green	All links are active.
One green; one red	One link is active, and at least one link is down or blocked.
Both red	All links are down or blocked.

The color of a device label shows the cluster membership of the device (Table 2-13).

Table 2-13 Device Label Colors

Label Color	Color Meaning
Green	A cluster member, either a member switch or the command switch
Cyan	A candidate switch that is eligible to join the cluster
Yellow	An unknown device or a device that is not eligible to join the cluster

Topology Display Options

You can set the type of information displayed in the Topology view by changing the settings in the Topology Options window. To display this window, select **View** > **Topology Options**. From this window, you can select:

- Device icons to be displayed in the Topology view
- Labels to be displayed with the device and link icons

Menus and Toolbar

The configuration and monitoring options for configuring switches and switch clusters are available from the menu bar, toolbar, and the Front-Panel and Topology view popup menus.

Menu Bar

The menu bar provides the complete list of options for managing a single switch and switch cluster. The menu bar is the same whether or not the Front-Panel or Topology views are displayed.

Options displayed from the menu bar can vary:

- The option for enabling a command switch is only available from a CMS session launched from a command-capable switch.
- Cluster management tasks, such as upgrading the software of groups of switches, are available only from a CMS session launched from a command switch.
- If you launch CMS from a specific switch, the menu bar displays the features supported only by that switch.
- If you launch CMS from a command switch, the menu bar displays the features supported on the switches in the cluster, with these exceptions:
  - If the command switch is a Layer 3 switch, such as a Catalyst 3550 switch, the menu bar displays the features of all Layer 3 and Layer 2 switches in the cluster.
  - If the command switch is a Layer 2 switch, such as a Catalyst 2950 or Catalyst 3500 XL switch, the menu bar displays the features of all Layer 2 switches in the cluster. The menu bar does not display Layer 3 features even if the cluster has Catalyst 3550 Layer 3 member switches.

Note We strongly recommend that the highest-end, command-capable switch in the cluster be the command switch so that all of the features supported in the cluster are displayed from the menu bar. If you have a switch cluster with a Catalyst 3550, that switch should be the command switch. If your switch cluster has Catalyst 2900 XL, Catalyst 2950, and Catalyst 3500 XL switches, the Catalyst 2950 should be the command switch. Refer to the release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm) for the Catalyst switches that can be part of a switch cluster.

Note

- Unless noted otherwise, Table 2-14 lists the menu-bar options available from a Catalyst 2900 XL or Catalyst 3500 XL command switch and when the cluster contains *only* Catalyst 2900 XL and Catalyst 3500 XL member switches. The menu bar of the command switch displays all menu-bar options available from the cluster, including options from member switches from other cluster-capable switch platforms.
- The footnotes in the table describe the availability of an option based on your access mode in CMS: read-only (access level 1–14) and read-write (access level 15). For more information about CMS access modes, see the "Access Modes in CMS" section on page 2-33.

- If your cluster has these member switches running earlier software releases and if you have read-only access to these member switches, some configuration windows for those switches display incomplete information:
  - Catalyst 2900 XL or Catalyst 3500 XL member switches running Cisco IOS Release 12.0(5)WC2 or earlier
  - Catalyst 2950 member switches running Cisco IOS Release 12.0(5)WC2 or earlier
  - Catalyst 3550 member switches running Cisco IOS Release 12.1(6)EA1 or earlier

  For more information about this limitation, refer to the Catalyst 2900 XL and Catalyst 3500 XL release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm).
- These switches do not support CMS access modes:
  - Catalyst 1900 and Catalyst 2820
  - Catalyst 2900 XL switches with 4-MB CPU DRAM

  If these switches are in a cluster that is using CMS access levels, these switches appear as unavailable devices and cannot be configured from CMS.

Table 2-14 Menu Bar

Menu-Bar Options	Task
CMS	
Page Setup	Set default document printer properties to be used when printing from CMS.
Print Preview	View the way the CMS window or help file will appear when printed.
Print	Print a CMS window or help file.
Guide Mode/Expert Mode[1]	Select which interaction mode to use when you select a configuration option.
Preferences[2]	Set CMS display properties, such as polling intervals, the default views to open at startup, and the color of administratively shutdown ports.
Administration	
IP Addresses[2]	Configure IP information for a switch.
SNMP[2]	Enable and disable Simple Network Management Protocol (SNMP), enter community strings, and configure end stations as trap managers.
System Time[2]	Configure the system time or configure the Network Time Protocol (NTP).
Console Baud Rate[2]	Change the baud rate for the switch console port.
MAC Addresses[2]	Enter dynamic, secure, and static addresses in a switch address table. You can also define the forwarding behavior of static addresses.
ARP[2]	Display the device Address Resolution Protocol (ARP) table, and configure the ARP cache timeout setting.
Save Configuration[1]	Save the configuration for the cluster or switch to Flash memory.
Software Upgrade[1]	Upgrade the software for the cluster or a switch.
System Reload[1]	Reboot the switch with the latest installed software.

Table 2-14 Menu Bar (continued)

Menu-Bar Options	Task
Cluster	
Cluster Manager[3]	Launch a CMS session from the command switch.
Create Cluster[1 4]	Designate a command switch, and name a cluster.
Delete Cluster[1 5]	Delete a cluster.
Add to Cluster[1 5]	Add a candidate to a cluster.
Remove from Cluster[1 5]	Remove a member from the cluster.
Standby Command Switches[2 5]	Create a Hot Standby Router Protocol (HSRP) standby group to provide command-switch redundancy.
Hop Count[2 5]	Enter the number of hops away that a command switch looks for members and for candidate switches.
Device	
Device Manager[5]	Launch Device Manager for a specific switch.
Host Name[1]	Change the host name of a switch.
STP[2]	Display and configure STP parameters for a switch.
CGMP[2]	Enable and disable the CGMP and the CGMP Fast Leave feature on a switch.
LRE Profiles	Display the LRE profile settings for the Catalyst 2900 LRE XL switches, and configure the speed of the LRE link.
AVVID Wizards[1]	Voice Wizard[1]—Configure a port to forward voice traffic with an 802.1P priority and configure the port as an 802.1Q trunk and as a member of the voice VLAN (VVID).
Port	
Port Settings[2]	Display and configure port parameters on a switch.
Port Search	Search for a port through its description.
Port Security[1]	Enable port security on a port.
EtherChannels[2]	Group ports into logical units for high-speed links between switches.
SPAN[2]	Enable Switch Port Analyzer (SPAN) port monitoring.
Protected Port[2]	Configure a port to prevent it from receiving bridged traffic from another port on the same switch.
Flooding Control[2]	Block the normal flooding of unicast and multicast packets, and enable the switch to block packet storms.
VLAN	
VLAN[2] (guide mode available[1])	Display VLAN membership, assign ports to VLANs, and configure Inter-Switch Link (ISL) and 802.1Q trunks. Display and configure the VLAN Trunking Protocol (VTP) for interswitch VLAN membership.
Management VLAN[2]	Change the management VLAN on the switch.
VMPS[2]	Configure the VLAN Membership Policy Server (VMPS).
Voice VLAN[2]	Configure a port to use a voice VLAN for voice traffic, separating it from the VLANs for data traffic.

Table 2-14 Menu Bar (continued)

Menu-Bar Options	Task
Reports	
Inventory	Display the device type, software version, IP address, and other information about a switch.
Port Statistics	Display port statistics.
Bandwidth Graphs	Display graphs that plot the total bandwidth in use by the switch.
Link Graphs	Display a graph showing the bandwidth being used for the selected link.
Link Reports	Display the link report for two connected devices. If one device is an unknown device or a candidate, only the cluster-member side of the link displays.
System Messages	Display the most recent system messages (IOS messages and switch-specific messages) sent by the switch software. This option is available on the Catalyst 2950 or Catalyst 3550 switches. It is not available from the Catalyst 2900 XL and Catalyst 3500 XL switches. You can display the system messages of the Catalyst 2900 XL and Catalyst 3500 XL switches when they are in a cluster where the command switch is a Catalyst 2950 switch running Cisco IOS Release 12.1(6)EA2 or later. For more information about system messages, see Appendix A, "System Messages."
View	
Refresh	Update the views with the latest status.
Front Panel	Display the Front Panel view.
Arrange Front Panel[1 5]	Rearrange the order in which switches appear in the Front Panel view.
Topology[5]	Display the Topology view.
Topology Options [5]	Select the information to be displayed in the Topology view.
Automatic Topology Layout[5]	Request CMS to rearrange the topology layout.
Save Topology Layout[1 5]	Save the presentation of the cluster icons that you arranged in the Topology view to Flash memory.
Window	List the open windows in your CMS session.

Table 2-14 Menu Bar (continued)

Menu-Bar Options	Task
Help	
Overview	Obtain an overview of the CMS interface.
What's New	Obtain a description of the new CMS features.
Help For Active Window	Display the help for the active open window. This is the same as clicking **Help** from the active window.
Contents	List all of the available online help topics.
Legend	Display the legend that describes the icons, labels, and links.
About	Display the CMS version number.

1. Not available in read-only mode. For more information about the read-only and read-write access modes, see the "Access Modes in CMS" section on page 2-33.
2. Some options from this menu option are not available in read-only mode.
3. Available only from a Device Manager session on a cluster member.
4. Available only from a Device Manager session on a command-capable switch that is not a cluster member.
5. Available only from a cluster management session.

Toolbar

The toolbar buttons display commonly used switch and cluster configuration options and information windows such as legends and online help. Hover the cursor over an icon to display the feature. Table 2-15 describes the toolbar options, from left to right on the toolbar.

Table 2-15 Toolbar Buttons

Toolbar Option	Keyboard Shortcut	Task
Print	Ctrl-P	Print a CMS window or help file.
Preferences[1]	Ctrl-R	Set CMS display properties, such as polling intervals, the views to open at CMS startup, and the color of administratively shutdown ports.
Save Configuration[2]	Ctrl-S	Save the configuration for the cluster or switch to Flash memory.
Software Upgrade[2]	Ctrl-U	Upgrade the software for the cluster or a switch.
Port Settings[1]	–	Display and configure port parameters on a switch.
VLAN[1]	–	Display VLAN membership, assign ports to VLANs, and configure ISL and 802.1Q trunks.
Inventory	–	Display the device type, the software version, the IP address, and other information about a switch.
Refresh	–	Update the views with the latest status.
Front Panel	–	Display the Front Panel view.
Topology[3]	–	Display the Topology view.
Topology Options[3]	–	Select the information to be displayed in the Topology view.
Save Topology Layout[2] [3]	–	Save the presentation of the cluster icons that you arranged in the Topology view to Flash memory.
Legend	–	Display the legend that describes the icons, labels, and links.
Help For Active Window	F1 key	Display the help for the active open window. This is the same as clicking **Help** from the active window.

1. Some options from this menu option are not available in read-only mode.
2. Not available in read-only mode. For more information about the read-only and read-write access modes, see the "Access Modes in CMS" section on page 2-33.
3. Available only from a cluster-management session.

Front Panel View Popup Menus

These popup menus are available in the Front Panel view.

Device Popup Menu

You can display all switch and cluster configuration windows from the menu bar, or you can display commonly used configuration windows from the device popup menu (Table 2-16). To display the device popup menu, click the switch icon from the cluster tree or the front-panel image itself, and right-click.

Table 2-16 Device Popup Menu

Popup Menu Option	Task
Device Manager[1]	Launch Device Manager for the switch.
Delete Cluster[2 3 4]	Delete a cluster.
Remove from Cluster[3 4]	Remove a member from the cluster.
Bandwidth Graphs	Display graphs that plot the total bandwidth in use.
Host Name[4]	Change the name of the switch.
Properties	Display information about the device and port on either end of the link and the state of the link.

1. Available from a cluster member switch but not from the command switch.
2. Available only from the command switch.
3. Available only from a cluster-management session.
4. Not available in read-only mode. For more information about the read-only and read-write access modes, see the "Access Modes in CMS" section on page 2-33.

Port Popup Menu

You can display all port configuration windows from the **Port** menu on the menu bar, or you can display commonly used port configuration windows from the port popup menu (Table 2-17). To display the port popup menu, click a specific port image, and right-click.

Table 2-17 Port Popup Menu

Popup Menu Option	Task
Port Settings[1]	Display and configure port settings.
VLAN[1]	Define the VLAN mode for a port or ports and add ports to VLANs. Not available for the Catalyst 1900 and Catalyst 2820 switches.
Port Security[1 2]	Enable port security on a port.
Link Graphs[3]	Display a graph showing the bandwidth used by the selected link.
Select All Ports	Select all ports on the switch for global configuration.

1. Some options from this menu option are not available in read-only mode.
2. Available on switches that support the Port Security feature.
3. Available only when there is an active link on the port (that is, the port LED is green when in port status mode).

Topology View Popup Menus

These popup menus are available in the Topology view.

Link Popup Menu

You can display reports and graphs for a specific link displayed in the Topology view (Table 2-18). To display the link popup menu, click the link icon, and right-click.

Table 2-18 Link Popup Menu

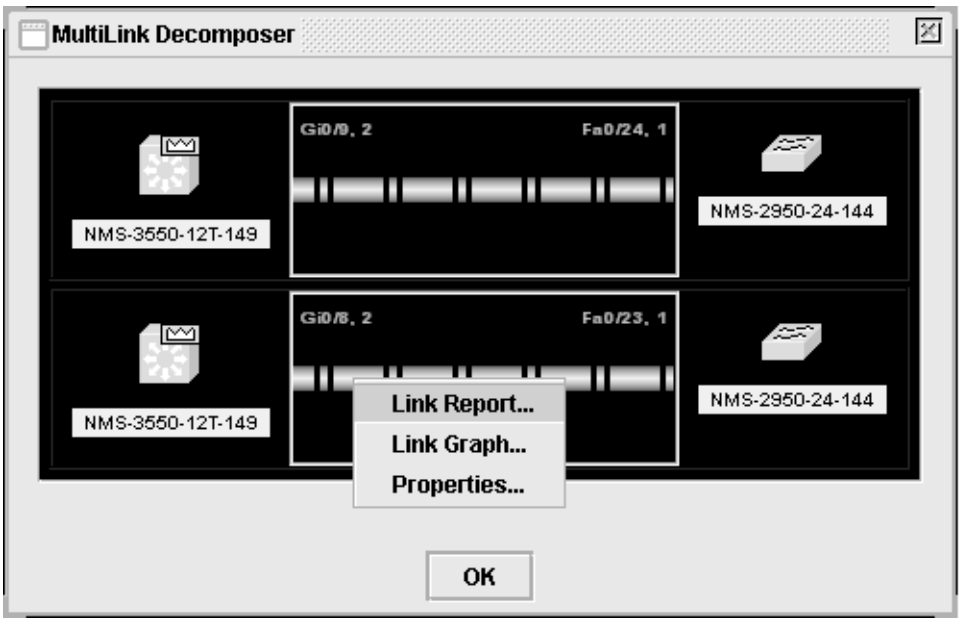
Popup Menu Option	Task
Link Report	Display the link report for two connected devices. If one device is an unknown device or a candidate, only the cluster member side of the link displays.
Link Graph	Display a graph showing the bandwidth used by the selected link.
Properties	Display information about the device and port on either end of the link and the state of the link.

The Link Report and Link Graph options are not available if at both ends of the link are

- Candidate switches
- Catalyst 1900 and Catalyst 2820 switches
- Devices that are not eligible to join the cluster

If multiple links are configured between two devices, when you click the link icon and right-click, the Multilink Content window appears (Figure 2-10). Click the link icon in this window, and right-click to display the link popup menu specific for that link.

Figure 2-10 Multilink Decomposer Window



Device Popup Menus

Specific devices in the Topology view display a specific popup menu:

- Cluster (Table 2-19)
- Command switch (Table 2-20)
- Member or standby command switch (Table 2-21)
- Candidate switch with an IP address (Table 2-22)
- Candidate switch without an IP address (Table 2-23)
- Neighboring devices (Table 2-24)

Note The Device Manager option in these popup menus is available in read-only mode on Catalyst 2900 XL and Catalyst 3500 XL switches running Cisco IOS Release 12.0(5)WC2 and later. It is also available on Catalyst 2950 switches running Cisco IOS Release 12.1(6)EA2 and later. It is not available on the Catalyst 1900 and Catalyst 2820 switches.

To display a device popup menu, click an icon, and right-click.

Table 2-19 Device Popup Menu of a Cluster Icon

Popup Menu Option	Task
Expand cluster	View a cluster-specific topology view.
Properties	Display information about the device and port on either end of the link and the state of the link.

Table 2-20 Device Popup Menu of a Command-Switch Icon

Popup Menu Option	Task
Collapse cluster	View the neighborhood outside a specific cluster.
Host Name[1]	Change the host name of a switch.
Bandwidth Graphs	Display graphs that plot the total bandwidth in use by the switch.
Properties	Display information about the device and port on either end of the link and the state of the link.

1. Not available in read-only mode. For more information about the read-only and read-write access modes, see the "Access Modes in CMS" section on page 2-33.

Table 2-21 Device Popup Menu of a Member or Standby Command-Switch Icon

Popup Menu Option	Task
Remove from Cluster[1]	Remove a member from the cluster.
Host Name[1]	Change the host name of a switch.
Device Manager[2]	Launch Device Manager for a switch.
Bandwidth Graphs	Display graphs that plot the total bandwidth in use by the switch.
Properties	Display information about the device and port on either end of the link and the state of the link.

1. Available only from a cluster-management session.
2. Available from a cluster member switch but not from the command switch.

Table 2-22 Device Popup Menu of a Candidate-Switch Icon (When the Candidate Switch Has an IP Address)

Popup Menu Option	Task
Add to Cluster[1]	Add a candidate to a cluster.
Device Manager[2]	Launch Device Manager for a switch.
Properties	Display information about the device and port on either end of the link and the state of the link.

1. Not available in read-only mode. For more information about the read-only and read-write access modes, see the "Access Modes in CMS" section on page 2-33.
2. Available from a cluster member switch but not from the command switch.

Table 2-23 Device Popup Menu of a Candidate-Switch Icon (When the Candidate Switch Does Not Have an IP Address)

Popup Menu Option	Task
Add to Cluster[1]	Add a candidate to a cluster.
Properties	Display information about the device and port on either end of the link and the state of the link.

1. Not available in read-only mode. For more information about the read-only and read-write access modes, see the "Access Modes in CMS" section on page 2-33.

Table 2-24 Device Popup Menu of a Neighboring-Device Icon

Popup Menu Option	Task
Device Manager[1]	Access the web management interface of the device. **Note** This option is available on Cisco access points, but not on Cisco IP phones, hubs, routers and on *unknown* devices such as some Cisco devices and third-party devices.
Disqualification Code	Display the reason why the device could not join the cluster.
Properties	Display information about the device and port on either end of the link and the state of the link.

1. Available from a cluster member switch but not from the command switch.

Interaction Modes

You can change the interaction mode of CMS to either guide or expert mode. Guide mode steps you through each feature option and provides information about the parameter. Expert mode displays a configuration window in which you configure the feature options.

Guide Mode

Note Guide mode is not available if your switch access level is read-only. For more information about the read-only access mode, see the "Access Modes in CMS" section on page 2-33.

Guide mode is for users who want a step-by-step approach for completing a specific configuration task. This mode is not available for all features. A menu-bar option that has a person icon means that guide mode is available for that option.

When you click **Guide Mode** and then select a menu-bar option that supports guide mode, CMS displays a specific parameter of the feature with information about the parameter field. To configure the feature, you provide the information that CMS requests in each step until you click **Finish** in the last step. Clicking **Cancel** at any time closes and ends the configuration task without applying any changes.

If **Expert Mode** is selected and you want to use guide mode, you must click **Guide Mode** before selecting an option from the menu bar, tool bar, or popup menu. If you change the interaction mode after selecting a configuration option, the mode change does not take effect until you select another configuration option.

Expert Mode

Expert mode is for users who prefer to display all the parameter fields of a feature in a single CMS window. Information about the parameter fields are provided from **Help**.

Wizards

Note Wizards are not available if your switch access level is read-only. For more information about the read-only access mode, see the "Access Modes in CMS" section on page 2-33.

Wizards simplify some configuration tasks on the switch. Similar to the guide mode, wizards provide a step-by-step approach for completing a specific configuration task. Unlike guide mode, a wizard does not prompt you to provide information for all of the feature options. Instead, it prompts you to provide minimal information and then uses the default settings of the remaining options to set up default configurations.

Wizards are not available for all features. A menu-bar option that has *wizard* means that selecting that option launches the wizard for that feature.

Tool Tips

CMS displays a popup message when you move your mouse over these devices:

- A yellow device icon in the cluster tree or in Topology view—A popup displays a fault message, such as that the RPS is faulty or that the switch is unavailable because you are in read-only mode.
- A red device icon in the cluster tree or in Topology view—A popup displays a message that the switch is down.

If you move your mouse over a table column heading, a popup displays the full heading.

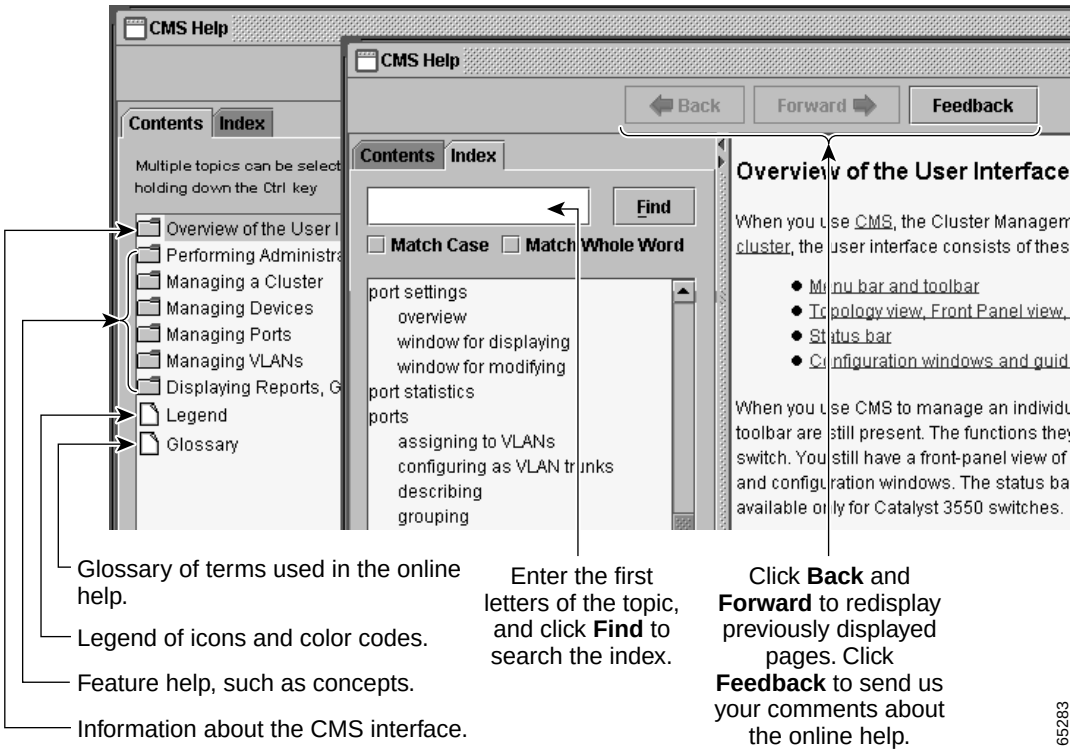
Online Help

CMS provides comprehensive online help to assist you in understanding and performing configuration and monitoring tasks from the CMS windows (Figure 2-11).

- Feature help, available from the menu bar by selecting **Help** > **Contents**, provides background information and concepts on the features.
- Dialog-specific help, available from **Help** on the CMS windows, provides procedures for performing tasks.
- Index of help topics.
- Glossary of terms used in the online help.

You can send us feedback about the information provided in the online help. Click **Feedback** to display an online form. After completing the form, click **Submit** to send your comments to Cisco. We appreciate and value your comments.

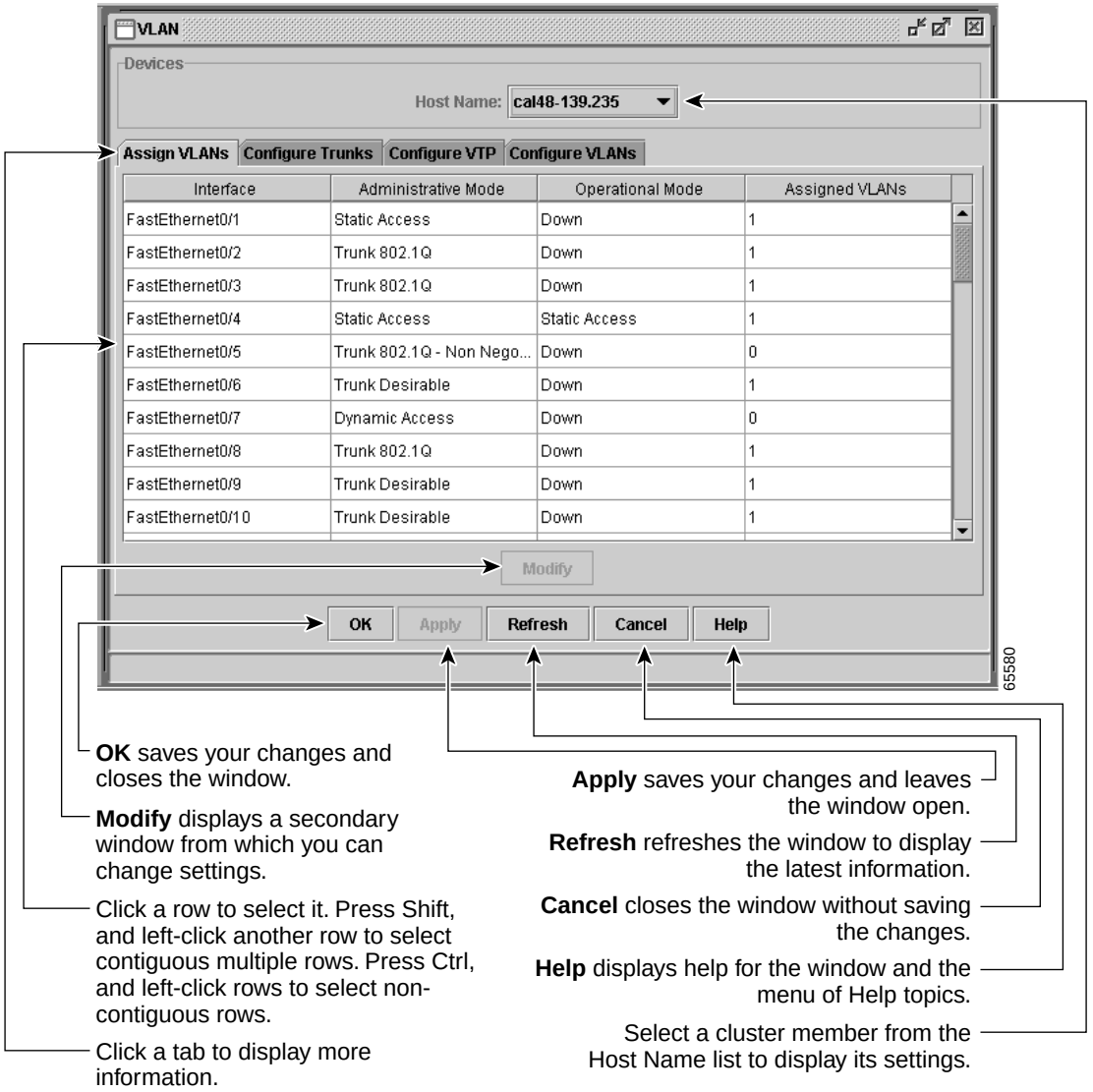
Figure 2-11 Help Contents and Index



CMS Window Components

CMS windows consistently present configuration information. Figure 2-12 shows the components of a typical CMS window.

Figure 2-12 CMS Window Components


VLAN
Devices
Host Name: cal48-139.235
Assign VLANs
Configure Trunks
Configure VTP
Configure VLANs
Interface
Administrative Mode
Operational Mode
Assigned VLANs
FastEthernet0/1 Static Access Down 1
FastEthernet0/2 Trunk 802.1Q Down 1
FastEthernet0/3 Trunk 802.1Q Down 1
FastEthernet0/4 Static Access Static Access 1
FastEthernet0/5 Trunk 802.1Q - Non Nego... Down 0
FastEthernet0/6 Trunk Desirable Down 1
FastEthernet0/7 Dynamic Access Down 0
FastEthernet0/8 Trunk 802.1Q Down 1
FastEthernet0/9 Trunk Desirable Down 1
FastEthernet0/10 Trunk Desirable Down 1
Modify
OK
Apply
Refresh
Cancel
Help
65580
OK saves your changes and closes the window.
Modify displays a secondary window from which you can change settings.
Click a row to select it. Press Shift, and left-click another row to select contiguous multiple rows. Press Ctrl, and left-click rows to select non-contiguous rows.
Click a tab to display more information.
Apply saves your changes and leaves the window open.
Refresh refreshes the window to display the latest information.
Cancel closes the window without saving the changes.
Help displays help for the window and the menu of Help topics.
Select a cluster member from the Host Name list to display its settings.

Host Name List

To display or change the configuration of a cluster member, you need to select the specific switch from the Host Name drop-down list. The list appears in the configuration window of each feature and lists only the cluster members that support that feature. For example, the Host Name list on the VLAN window does not include Catalyst 1900 and Catalyst 2820 switches even though they are part of the cluster. Similarly, the Host Name list on the LRE Profiles window only lists the LRE switches in the cluster.

Tabs, Lists, and Tables

Some CMS windows have *tabs* that present different sets of information. Tabs are arranged like folder headings across the top of the window. Click the tab to display its information.

Listed information can often be changed by selecting an item from a list. To change the information, select one or more items, and click **Modify**. Changing multiple items is limited to those items that apply to at least one of the selections.

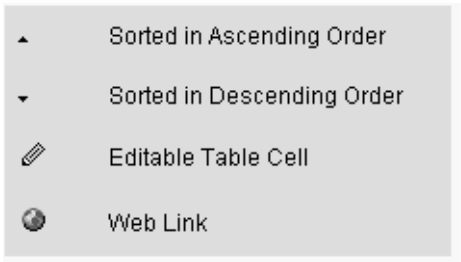
Some CMS windows present information in a table format. You can edit the information in these tables.

Note You can resize the width of the columns to display the column headings, or you can hover your cursor over the heading to display a popup description of the column.

Icons Used in Windows

Some window have icons for sorting information in tables, for showing which cells in a table are editable, and for displaying further information from Cisco.com (Figure 2-13).

Figure 2-13 Window Icons



Buttons

These are the most common buttons that you use to change the information in a CMS window:

- OK—Save any changes and close the window. If you made no changes, the window closes. If CMS detects errors in your entry, the window remains open. For more information about error detection, see the "Error Checking" section on page 2-34.
- Apply—Save any changes made in the window and leave the window open. If you made no changes, the Apply button is disabled.
- Refresh—Update the CMS window with the latest status of the device. Unsaved changes are lost.
- Cancel—Do not save any changes made in the window and close the window.
- Help—Display procedures on performing tasks from the window.
- Modify—Display the secondary window for changing information on the selected item or items. You usually select an item from a list or table and click **Modify**.

Accessing CMS

This section assumes the following:

- You know the IP address and password of the command switch or a specific switch. This information is either:
  - Assigned to the switch by following the setup program, as described in the release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm).
  - Changed on the switch by following the information in the "Changing IP Information" section on page 6-2 and "Assigning Passwords and Privilege Levels" section on page 6-11. Considerations for assigning IP addresses and passwords to a command switch and cluster members are described in the "IP Addresses" section on page 5-13 and "Passwords" section on page 5-14.
- You know your access privilege level to the switch.
- You have referred to the release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm) for system requirements and have followed the procedures for installing the required Java plug-ins and configuring your browser.

Caution Copies of the CMS pages you display are saved in your browser memory cache until you exit the browser session. A password is not required to redisplay these pages, including the Cisco Systems Access page. You can access the CLI by clicking **Web Console - HTML access to the command line interface** from a cached copy of the Cisco Systems Access page. To prevent unauthorized access to CMS and the CLI, exit your browser to end the browser session.

To access CMS, follow these steps:

Step 1 Enter the switch IP address and your privilege level in the browser **Location** field (Netscape Communicator) or Address field (Microsoft Internet Explorer). For example:

```
http://10.1.126.45:184/level/14/
```

where `10.1.126.45` is the switch IP address, `184` is the HTTP port, and level `14` is the privilege level. You do not need to enter the HTTP port if the switch is using HTTP port 80 (the default) or enter the privilege level if you have read-write access to the switch (privilege level is 15). For information about the HTTP port, see the "HTTP Access to CMS" section on page 4-5. For information about privilege levels, see the "Access Modes in CMS" section on page 2-33.

Step 2 When prompted for a username and password, enter only the switch enable password. CMS prompts you a second time for a username and password. Enter only the enable password again.

If you configure a local username and password, make sure you enable it by using the **ip http authentication** global configuration command. Enter your username and password when prompted.

Step 3 Click **Cluster Management Suite**.

If you access CMS from a standalone or member switch, Device Manager appears. If you access CMS from a command switch, you can display the Front Panel and Topology views.

Access Modes in CMS

CMS provides two levels of access to the configuration options: read-write access and read-only access. Privilege levels 0 to 15 are supported.

- Privilege level 15 provides you with read-write access to CMS.
- Privilege levels 1 to 14 provide you with read-only access to CMS. Any options in the CMS windows, menu bar, toolbar, and popup menus that change the switch or cluster configuration are not shown in read-only mode.
- Privilege level 0 denies access to CMS.

If you do not include a privilege level when you access CMS, the switch verifies if you have privilege-level 15. If you do not, you are denied access to CMS. If you do have privilege-level 15, you are granted read-write access. Therefore, you do not need to include the privilege level if it is 15. Entering zero denies access to CMS. For more information about privilege levels, see the "Assigning Passwords and Privilege Levels" section on page 6-11.

Note

- If your cluster has these member switches running earlier software releases and if you have read-only access to these member switches, some configuration windows for those switches display incomplete information:
  - Catalyst 2900 XL or Catalyst 3500 XL member switches running Cisco IOS Release 12.0(5)WC2 or earlier
  - Catalyst 2950 member switches running Cisco IOS Release 12.0(5)WC2 or earlier
  - Catalyst 3550 member switches running Cisco IOS Release 12.1(6)EA1 or earlier

  For more information about this limitation, refer to the Catalyst 2900 XL and Catalyst 3500 XL release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm).
- These switches do not support read-only mode on CMS:
  - Catalyst 1900 and Catalyst 2820
  - Catalyst 2900 XL switches with 4-MB CPU DRAM

  In read-only mode, these switches appear as unavailable devices and cannot be configured from CMS.

Verifying Your Changes

CMS provides notification cues to help you track and confirm the changes you make.

Change Notification

A green border around a field or table cell means that you made an unsaved change to the field or table cell. Previous information in that field or table cell is displayed in the window status bar. When you save the changes or if you cancel the change, the green border disappears.

Error Checking

A red border around a field means that you entered invalid data in the field. An error message also displays in the window status bar. When you enter valid data in the field, a green border replaces the red border until you either save or cancel the change.

If there is an error in communicating with the switch or if you make an error while performing an action, a popup dialog notifies you about the error.

Saving Your Changes

Note The Save Configuration option is not available if your switch access level is read-only. For more information about the read-only access mode, see the "Access Modes in CMS" section on page 2-33.

Tip As you make cluster configuration changes (except for changes to the Topology view and in the Preferences window), make sure that you periodically save the configuration from the command switch. The configuration is saved on the command and member switches.

The front-panel images and CMS windows always display the *running configuration* of the switch. When you make a configuration change to a switch or switch cluster, the change becomes part of the running configuration. The change *does not* automatically become part of the config.txt file in Flash memory, which is the *startup configuration* used each time the switch restarts. If you do not save your changes to Flash memory, they are lost when the switch restarts.

To save all configuration changes to Flash memory, you must select **Administration > Save Configuration**.

Note Catalyst 1900 and Catalyst 2820 switches automatically save configuration changes to Flash memory as they occur.

Using Different Versions of CMS

When managing switch clusters through CMS, remember that clusters can have a mix of switch models using different IOS releases and that CMS in earlier IOS releases and on different switch platforms might look and function differently from CMS in this IOS release.

When you select **Device > Device Manager** for a cluster member, a new browser session is launched, and the CMS version for that switch is displayed.

Here are examples of how CMS can differ between IOS releases and switch platforms:

- On Catalyst switches running Cisco IOS Release 12.0(5)WC2 or earlier or Cisco IOS Release 12.1(6)EA1 or earlier, the CMS versions in those software releases might appear similar but are not the same as this release. For example, the Topology view in this release is not the same as the Topology view or Cluster View in those earlier software releases.
- CMS on the Catalyst 1900 and Catalyst 2820 switches is referred to as *Switch Manager*. Cluster management options are not available on these switches. This is the earliest version of CMS.

Refer to the documentation specific to the switch and its IOS release for descriptions of the CMS version you are using.

Where to Go Next

The rest of this guide provides information about and CLI procedures for the software features supported in this release. For CMS procedures and window descriptions, refer to the online help.

Refer to the release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm) for:

- CMS software requirements
- Procedures for browser configuration
- Procedures for accessing CMS

Getting Started with the CLI

This chapter provides information that you should know before using the Cisco IOS command-line interface (CLI). If you have never used IOS software or if you need a refresher, take a few minutes to read this chapter before reading the rest of this guide.

- Command Usage Basics, page 3-2
- Command-Line Error Messages, page 3-6
- Accessing the CLI, page 3-7
- Saving Configuration Changes, page 3-8
- Where to Go Next, page 3-8

This switch software release is based on Cisco IOS Release 12.0. It has been enhanced to support a set of features for the Catalyst 2900 XL and Catalyst 3500 XL switches. This chapter provides procedures for using only the commands that have been created or changed for these switches. The *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference* provides complete descriptions of these commands. This chapter does not provide Cisco IOS Release 12.0 commands and information already documented in the Cisco IOS Release 12.0 documentation on Cisco.com.

Command Usage Basics

This section provides these topics:

- "Accessing Command Modes" section on page 3-2
- "Specifying Ports in Interface Configuration Mode" section on page 3-4
- "Abbreviating Commands" section on page 3-4
- "Using the No and Default Forms of Commands" section on page 3-5
- "Redisplaying a Command" section on page 3-5
- "Getting Help" section on page 3-5

For complete information about CLI usage, refer to the Cisco IOS Release 12.0 documentation on Cisco.com.

Accessing Command Modes

The Cisco IOS CLI is divided into different modes. The commands available to you at any given time depend on which mode you are in. Entering a question mark (**?**) at the system prompt provides a list of commands for each command mode.

When you start a session on the switch, you begin in user mode, often called user EXEC mode. Only a limited subset of the commands are available in user EXEC mode. For example, most of the user EXEC commands are one-time commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. The user EXEC commands are not saved when the switch reboots.

To have access to all commands, you must enter privileged EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. From this mode, you can enter any privileged EXEC command or enter global configuration mode.

Using the configuration modes (such as global, VLAN, and interface), you can make changes to the running configuration. If you save the configuration, these commands are stored when the switch reboots. To access the various configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and line configuration mode.

Table 3-1 describes the *main* command modes supported on the switch, the prompt you see in that mode, and how to exit the mode. The examples in the table use the host name *switch*.

Table 3-1 Command Modes Summary

Modes	Access Method	Prompt	Exit Method	About This Mode[1]
User EXEC	Begin a session with your switch.	`switch>`	Enter **logout** or **quit**.	Use this mode to • Change terminal settings. • Perform basic tests. • Display system information.
Privileged EXEC	Enter the **enable** command while in user EXEC mode.	`switch#`	Enter **disable** to exit.	Use this mode to verify commands you have entered. Use a password to protect access to this mode.
Global configuration	Enter the **configure** command while in privileged EXEC mode.	`switch(config)#`	To exit to privileged EXEC mode, enter **exit** or **end**, or press **Ctrl-Z**.	Use this mode to configure parameters that apply to your switch as a whole.
VLAN database	Enter the **vlan database** command while in privileged EXEC mode.	`switch(vlan)#`	To exit to privileged EXEC mode, enter **exit**.	Use this mode to configure VLAN-specific parameters.
Interface configuration	Enter the **interface** command (with a specific interface) while in global configuration mode.	`switch(config-if)#`	To exit to global configuration mode, enter **exit**. To exist to privileged EXEC mode, enter **Ctrl-Z or end.**	Use this mode to configure parameters for the Ethernet interfaces.
Line configuration	Specify a line with the **line vty** or **line console** command while in global configuration mode.	`switch(config-line)#`	To exit to global configuration mode, enter **exit**. To exit to privileged EXEC mode, enter **Ctrl-Z or end.**	Use this mode to configure parameters for the terminal line.

1. For any of the modes, you can see a comprehensive list of the available commands by entering a question mark (**?**) at the prompt.

Specifying Ports in Interface Configuration Mode

To configure a port, you need to specify the interface type, slot, and switch-port number with the **interface** configuration command. For example, to configure port 4 on a switch, you enter:

```
switch(config)#interface fa 0/4
```

To configure port 4 on a 10/100 module in the first module slot on the switch, you enter:

```
switch(config)#interface fa 1/4
```

- Interface type—Each switch in the Catalyst 2900 series XL and Catalyst 3500 series XL platform supports different types of interfaces. To display a complete list of the interface types supported on your switch, enter the **interface ?** command from the global configuration mode. This example shows what the **interface ?** command displays on a Catalyst 2900 LRE XL switch:

```
lreswitch(config)#interface ?
  FastEthernet       FastEthernet IEEE 802.3
  LongReachEthernet  Ethernet over VDSL
  Multilink          Multilink-group interface
  Port-channel       Ethernet Channel of interfaces
  VLAN               Switch VLAN Virtual Interface
  Virtual-TokenRing  Virtual TokenRing
```

Note The multilink, port-channel, and virtual-TokenRing interface types are not supported on the Catalyst 2900 XL and Catalyst 3500 XL switches.

- Slot number—The slot number on the switch. On the modular Catalyst 2900 XL switches, the slot number is 1 or 2. On non-modular Catalyst 2900 XL and Catalyst 3500 XL switches, the slot number is 0.
- Port number—The number of the physical port on the switch. Refer to your switch for the port numbers.

Abbreviating Commands

You only have to enter enough characters for the switch to recognize the command as unique. This example shows how to enter the **show configuration** command:

```
Switch# show conf
```

Using the No and Default Forms of Commands

Almost every configuration command has a **no** form. In general, use the **no** form to

- Disable a feature or function.
- Reset a command to its default values.
- Reverse the action of a command. For example, the **no shutdown** command reverses the shutdown of an interface.

Use the command without the **no** form to reenable a disabled feature or to reverse the action of a **no** command.

Configuration commands can also have a **default** form. The **default** form of a command returns the command setting to its default. Most commands are disabled by default, so the **default** form is the same as the **no** form. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** command enables the command and sets variables to their default values.

Redisplaying a Command

To redisplay a command you previously entered, press the up-arrow key. You can continue to press the up-arrow key for more commands.

Getting Help

Entering a question mark (**?**) at the system prompt displays a list of commands for each command mode.When using context-sensitive help, the space (or lack of a space) before the question mark (**?**) is significant. To obtain a list of commands that begin with a particular character sequence, enter those characters followed immediately by the question mark (**?**). Do not include a space. This form of help is called word help, because it completes a word for you.

To list keywords or arguments, enter a question mark (**?**) in place of a keyword or argument. Include a space before the **?**. This form of help is called command syntax help, because it reminds you which keywords or arguments are applicable based on the command, keywords, and arguments you already have entered.

You can also obtain a list of associated keywords and arguments for any command, as shown in Table 3-2.

Table 3-2 Help Summary

Command	Purpose
help	Obtain a brief description of the help system in any command mode.

*abbreviated-command-entry***?**	Obtain a list of commands that begin with a particular character string.
	For example:
	`Switch# di?`
	`dir  disable  disconnect`

abbreviated-command-entry<**Tab**>	Complete a partial command name.
	For example:
	`Switch# sh conf<tab>`
	`Switch# show configuration`

?	List all commands available for a particular command mode. For example: `Switch> ?`
command **?**	List the associated keywords for a command. For example: `Switch> show ?`

command keyword **?**	List the associated arguments for a keyword.
	For example:
	`Switch(config)# cdp holdtime ?`
	`  <10-255>  Length of time (in sec) that receiver must keep this packet`

Command-Line Error Messages

Table 3-3 lists some error messages that you might encounter while using the CLI.

Table 3-3 Common CLI Error Messages

Error Message	Meaning	How to Get Help
`% Ambiguous command: "show con"`	You did not enter enough characters for your switch to recognize the command.	Reenter the command followed by a space and a question mark (**?**). The possible keywords that you can enter with the command appear.
`% Incomplete command.`	You did not enter all of the keywords or values required by this command.	Reenter the command followed by a space and a question mark (**?**). The possible keywords that you can enter with the command appear.
`% Invalid input detected at '^' marker.`	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (**?**) to display all of the commands that are available in this command mode. The possible keywords that you can enter with the command appear.

Accessing the CLI

This procedure assumes you have already assigned IP information and password to the switch or command switch. You can assign this information to the switch in these ways:

- Using the setup program, as described in the release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm).
- Manually assigning an IP address and password, as described in the "Changing IP Information" section on page 6-2 and "Assigning Passwords and Privilege Levels" section on page 6-11.

  Considerations for assigning this information to a command switch and cluster members are described in the "IP Addresses" section on page 5-13 and "Passwords" section on page 5-14.

To access the CLI from a terminal session, follow these steps:

Step 1 Start up the emulation software (such as ProComm, HyperTerminal, tip, or minicom) on the management station.

Step 2 If necessary, reconfigure the terminal-emulation software to match the switch console port settings (default settings are 9600 baud, no parity, 8 data bits, and 1 stop bit).

Step 3 Establish a connection with the switch by either

- Connecting the switch console port to a management station or dial-up modem. For information about connecting to the console port, refer to the switch hardware installation guide.
- Using any Telnet TCP/IP package from a remote management station. The switch must have network connectivity with the Telnet client, and the switch must have an enable secret password configured. For information about configuring the switch for Telnet access, see the "SNMP Network Management Platforms" section on page 4-5.

  The switch supports up to seven simultaneous Telnet sessions. Changes made by one Telnet user are reflected in all other Telnet sessions.

After you connect through the console port or through a Telnet session, the User EXEC prompt appears on the management station.

Accessing the CLI from a Browser

This procedure assumes you have met the software requirements, (including browser and Java plug-in configurations) and have assigned IP information and a Telnet password to the switch or command switch, as described in the release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm).

Caution Copies of the CMS pages you display are saved in your browser memory cache until you exit the browser session. A password is not required to redisplay these pages, including the Cisco Systems Access page. You can access the CLI by clicking **Web Console - HTML access to the command line interface** from a cached copy of the Cisco Systems Access page. To prevent unauthorized access to CMS and the CLI, exit your browser to end the browser session.

To access the CLI from a web browser, follow these steps:

Step 1 Start one of the supported browsers.

Step 2 In the **URL** field, enter the IP address of the command switch.

Step 3 When the Cisco Systems Access page appears, click **Telnet** to start a Telnet session.

You can also access the CLI by clicking **Web Console - HTML access to the command line interface** from the Cisco Systems Access page. For information about the Cisco Systems Access page, see the "Accessing CMS" section on page 2-32 and the release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm).

Step 4 Enter the switch password.

The User EXEC prompt appears on the management station.

Saving Configuration Changes

The **show** command always displays the *running configuration* of the switch. When you make a configuration change to a switch or switch cluster, the change becomes part of the running configuration. The change *does not* automatically become part of the config.txt file in Flash memory, which is the *startup configuration* used each time the switch restarts. If you do not save your changes to Flash memory, they are lost when the switch restarts.

To save all configuration changes to Flash memory, you must enter the **write memory** command in privileged EXEC mode.

Note The **write memory** command does not apply to the Catalyst 1900 and Catalyst 2820 switches, which automatically save configuration changes to Flash memory as they occur.

Tip As you make cluster configuration changes, make sure you periodically save the configuration. The configuration is saved on the command and member switches.

Where to Go Next

The rest of this guide provides information about and CLI procedures for the software features supported in this release. For CMS procedures and window descriptions, refer to the online help.

Refer to the release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm) for this information:

- CMS software requirements
- Procedures for browser configuration
- Procedures for accessing CMS

General Switch Administration

This chapter provides these switch administration topics:

- Basic IP Connectivity to the Switch, page 4-2
- Switch Software Releases, page 4-2
- Console Port Access, page 4-3
- Telnet Access to the CLI, page 4-4
- HTTP Access to CMS, page 4-5
- SNMP Network Management Platforms, page 4-5
- Default Settings, page 4-8

The following information tends to change and therefore appear only in the release notes. Before installing, configuring, or upgrading the switch, refer to the release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm) for the latest information about:

- Software and hardware requirements and compatibility
- Browser and Java plug-in configurations
- Setup program
- Switch upgrades

This switch software release is based on Cisco IOS Release 12.0. It has been enhanced to support a set of features for the Catalyst 2900 XL and Catalyst 3500 XL switches. This chapter provides procedures for using only the commands that have been created or changed for these switches. The *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference* provides complete descriptions of these commands. This chapter does not provide Cisco IOS Release 12.0 commands and information already documented in the Cisco IOS Release 12.0 documentation on Cisco.com.

Basic IP Connectivity to the Switch

The switch uses IP address information to communicate with the local routers and the Internet. You need assign an IP address to the switch if you plan to use CMS to configure and manage the switch. The switch also requires a secret password. IP information is

- Switch IP address
- Subnet mask (IP netmask)
- Default gateway (router)

The first time that you access the switch, it runs a setup program that prompts you to assign basic information (such as IP address and passwords) to the switch. For information about running the setup program, refer to the latest switch release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm).

Once IP information is assigned, you can run the switch on its default settings or configure any settings to meet your network requirements.

For more information about IP information, see the "Changing IP Information" section on page 6-2. For more information about passwords, see the "Accessing CMS" section on page 2-32 and "Assigning Passwords and Privilege Levels" section on page 6-11.

Switch Software Releases

The switch software is regularly updated with new features and bug fixes, and you might want to upgrade your Catalyst 2900 XL and Catalyst 3500 XL with the latest software release. New software releases are posted on Cisco.com on the World Wide Web and are available through authorized resellers. Cisco also supplies a TFTP server that you can download from Cisco.com.

Before upgrading a switch, first find out the version of the software that the switch is running. You can do this by using the Software Upgrade window, by selecting **Help > About**, or by using the **show version** command.

Knowing the software version is also important for compatibility reasons, especially for switch clusters. Refer to the latest switch release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm) for this information:

- Compatibility requirements
- Upgrade guidelines and procedures and software reload information

Console Port Access

The switch console port provides switch access to a directly-attached terminal or PC or to a remote terminal or PC through a serial connection and a modem. For information about connecting to the switch console port, refer to the switch hardware installation guide.

Be sure that the switch console port settings match the settings of the terminal or PC. These are the default settings of the switch console port:

- Baud rate default is 9600.
- Data bits default is 8.

Note If the data bits option is set to 8, set the parity option to None.

- Stop bits default is 1.
- Parity settings default is None.

Make sure that you save any changes you make to the switch console port settings to Flash memory. For information about saving changes from CMS, see the "Saving Your Changes" section on page 2-34. For information about saving changes from the CLI, see the "Saving Configuration Changes" section on page 3-8.

Telnet Access to the CLI

This procedure assumes that you have assigned IP information and a Telnet password to the switch or command switch, as described in the latest switch release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm). Information about accessing the CLI through a Telnet session is provided in the "Accessing the CLI" section on page 3-7.

To configure the switch for Telnet access, follow these steps:

	Command	Purpose
Step 1		Attach a PC or workstation with emulation software to the switch console port. The default data characteristics of the switch console port are 9600, 8, 1, no parity. When the command line appears, go to Step 2.
Step 2	**enable**	Enter privileged EXEC mode.
Step 3	**config terminal**	Enter global configuration mode.
Step 4	**line vty 0 15**	Enter the interface configuration mode for the Telnet interface. There are 16 possible sessions on a command-capable switch. The 0 and 15 mean that you are configuring all 16 possible Telnet sessions.
Step 5	**password** <*password*>	Enter a enable secret password. For more information about passwords, see the "Assigning Passwords and Privilege Levels" section on page 6-11.
Step 6	**end**	Return to privileged EXEC mode so that you can verify the entry.
Step 7	**show running-config**	Display the running configuration. The password is listed under the command **line vty 0 15**.
Step 8	**copy running-config startup-config**	(Optional) Save the running configuration to the startup configuration.

HTTP Access to CMS

CMS uses Hypertext Transfer Protocol (HTTP), which is an in-band form of communication with the switch through any one of its Ethernet ports and that allows switch management from a standard web browser. The default HTTP port is 80.

If you change the HTTP port, you must include the new port number when you enter the IP address in the browser **Location** or **Address** field (for example, http://10.1.126.45:184 where 184 is the new HTTP port number).

Do not disable or otherwise misconfigure the port through which your management station is communicating with the switch. You might want to write down the port number to which you are connected. Changes to the switch IP information should be done with care.

For information about connecting to a switch port, refer to the switch hardware installation guide.

SNMP Network Management Platforms

You can manage switches by using an Simple Network Management Protocol (SNMP)-compatible management station running such platforms as HP OpenView or SunNet Manager. CiscoWorks2000 and CiscoView 5.0 are network-management applications you can use to configure, monitor, and troubleshoot Catalyst 2900 XL and Catalyst 3500 XL switches.

The switch supports a comprehensive set of Management Information Base (MIB) extensions and MIB II, the IEEE 802.1D bridge MIB, and four Remote Monitoring (RMON) groups, which this IOS software release supports. You can configure these groups by using an SNMP application or by using the CLI. The four supported groups are alarms, events, history, and statistics.

This section describes how to access MIB objects to configure and manage your switch. It provides this information:

- Using File Transfer Protocol (FTP) to access the MIB files
- Using SNMP to access the MIB variables

For more information about SNMP, see the "Configuring SNMP" section on page 6-48.

In a cluster configuration, the command switch manages communication between the SNMP management station and all switches in the cluster. For information about managing cluster switches through SNMP, see the "Using SNMP to Manage Switch Clusters" section on page 5-25.

When configuring your switch by using SNMP, note that certain combinations of port features create configuration conflicts. For more information, see the "Avoiding Configuration Conflicts" section on page 9-2.

Using FTP to Access the MIB Files

You can obtain each MIB file with this procedure:

Step 1 Use FTP to access the server **ftp.cisco.com**.

Step 2 Log in with the username *anonymous*.

Step 3 Enter your e-mail username when prompted for the password.

Step 4 At the `ftp>` prompt, change directories to /pub/mibs/supportlists.

Step 5 Change directories to one of the following:

- **wsc2900xl** for a list of Catalyst 2900 XL MIBs
- **wsc3500xl** for a list of Catalyst 3500 XL MIBs

Step 6 Use the **get** *MIB_filename* command to obtain a copy of the MIB file.

You can also access this server from your browser by entering this URL in the **Location** field of your Netscape browser (the **Address** field in Internet Explorer):

`ftp://ftp.cisco.com`

Use the mouse to navigate to the folders listed above.

Using SNMP to Access MIB Variables

The switch MIB variables are accessible through SNMP, an application-layer protocol facilitating the exchange of management information between network devices. The SNMP system consists of three parts:

- The SNMP manager, which resides on the network management system (NMS)
- The SNMP agent, which resides on the switch
- The MIBs that reside on the switch but that can be compiled with your network management software

An example of an NMS is the CiscoWorks network management software. CiscoWorks2000 software uses the switch MIB variables to set device variables and to poll devices on the network for specific information. The results of a poll can be displayed as a graph and analyzed to troubleshoot internetworking problems, increase network performance, verify the configuration of devices, monitor traffic loads, and more.

As shown in Figure 4-1, the SNMP agent gathers data from the MIB, which is the repository for information about device parameters and network data. The agent can send traps, or notification of certain events, to the SNMP manager, which receives and processes the traps. Traps are messages alerting the SNMP manager to a condition on the network such as improper user authentication, restarts, link status (up or down), and so forth. In addition, the SNMP agent responds to MIB-related queries sent by the SNMP manager in *get-request*, *get-next-request*, and *set-request* format.

The SNMP manager uses information in the MIB to perform the operations described in Table 4-1.

Figure 4-1 SNMP Network

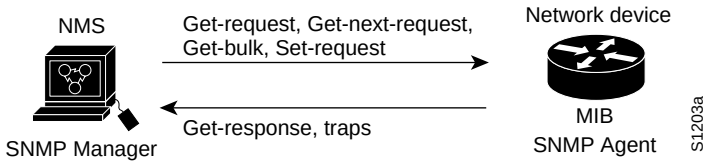


Table 4-1 SNMP Operations

Operation	Description
get-request	Retrieves a value from a specific variable.
get-next-request	Retrieves a value from a variable within a table.[1]
get-bulk-request[2]	Retrieves large blocks of data, such as multiple rows in a table, which would otherwise require the transmission of many small blocks of data.
get-response	Replies to a get-request, get-next-request, and set-request sent by an NMS.
set-request	Stores a value in a specific variable.
trap	An unsolicited message sent by an SNMP agent to an SNMP manager indicating that some event has occurred.

1. With this operation, an SNMP manager does not need to know the exact variable name. A sequential search is performed to find the needed variable from within a table.
2. The **get-bulk** command only works with SNMP version 2.

Default Settings

The switch is designed for plug-and-play operation, requiring only that you assign basic IP information to the switch and connect it to the other devices in your network. For information about assigning basic IP information to the switch, see the "Basic IP Connectivity to the Switch" section on page 4-2 and the latest switch release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm).

If you have specific network needs, you can configure the switch through its various management interfaces. Table 4-2 lists the key software features, their defaults, their page numbers in this guide, and where you can configure them from the command-line interface (CLI) and Cluster Management Suite (CMS).

Table 4-2 Default Settings and Where to Change Them

Feature	Default Setting	Concepts and CLI Procedures	CMS Option
Cluster Management			
Enabling a command switch[1]	None	"Enabling a Command Switch" section on page 5-18. No CLI procedure provided. For the cluster commands, refer to the *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference*.	Device Manager (not within a cluster session) from a command-capable switch **Cluster > Create Cluster**
Creating a cluster[1]	None	"Creating a Switch Cluster" section on page 5-17. No CLI procedure provided. For the cluster commands, refer to the *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference*.	Device Manager (not within a cluster session) from a command-capable switch **Cluster > Create Cluster**
Adding and removing cluster members[2]	None	"Adding Member Switches" section on page 5-19. No CLI procedure provided. For the cluster commands, refer to the *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference*.	**Cluster > Add to Cluster** and **Cluster > Remove from Cluster**
Creating a standby command switch group[2]	None	"Creating a Cluster Standby Group" section on page 5-21. No CLI procedure provided. For the cluster commands, refer to the *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference*.	**Cluster > Standby Command Switches**
Upgrading cluster software	Enabled	"Switch Software Releases" section on page 4-2. Refer to the latest switch release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm).	**Administration > Software Upgrade**
Configuring SNMP community strings and trap managers	None	"SNMP Community Strings" section on page 5-14 and "Configuring SNMP" section on page 6-48.	**Administration > SNMP**

Table 4-2 Default Settings and Where to Change Them (continued)

Feature	Default Setting	Concepts and CLI Procedures	CMS Option
Device Management			
Switch IP address, subnet mask, and default gateway	0.0.0.0	"Changing IP Information" section on page 6-2. Refer to the latest switch release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm). Documentation set for Cisco IOS Release 12.0 on Cisco.com.	**Administration > IP Addresses**
Dynamic Host Configuration Protocol (DHCP)	DHCP client is enabled	"Using DHCP-Based Autoconfiguration" section on page 6-3. Documentation set for Cisco IOS Release 12.0 on Cisco.com.	–
Domain name	None	"Configuring the Domain Name and the DNS" section on page 6-6. Documentation set for Cisco IOS Release 12.0 on Cisco.com.	**Administration > IP Addresses**
Cisco Discovery Protocol (CDP)	Enabled	"Configuring CDP" section on page 6-13. Documentation set for Cisco IOS Release 12.0 on Cisco.com.	**Cluster > Hop Count**
Address Resolution Protocol (ARP)	Enabled	"Managing the ARP Table" section on page 6-32. Documentation set for Cisco IOS Release 12.0 on Cisco.com.	**Administration > ARP**
System Time Management	None	"Setting the System Date and Time" section on page 6-12. Documentation set for Cisco IOS Release 12.0 on Cisco.com.	**Administration > System Time**
MAC address notification	Disabled	"MAC Address Notification" section on page 6-17.	–
Static address assignment	None assigned	"Adding Static Addresses" section on page 6-19. Documentation set for Cisco IOS Release 12.0 on Cisco.com.	**Administration > MAC Addresses**
Dynamic address management	Enabled	"Managing the MAC Address Tables" section on page 6-15. Documentation set for Cisco IOS Release 12.0 on Cisco.com.	**Administration > MAC Addresses**

Table 4-2 Default Settings and Where to Change Them (continued)

Feature	Default Setting	Concepts and CLI Procedures	CMS Option
Management VLAN	VLAN 1	"Management VLANs" section on page 8-3.	**VLAN > Management VLAN**
VLAN membership	Static-access ports in VLAN 1	"Assigning VLAN Port Membership Modes" section on page 8-5.	**VLAN > VLAN**
VMPS Configuration	–	"How the VMPS Works" section on page 8-35.	**VLAN > VMPS**
VTP Management	VTP server mode	"Configuring VTP" section on page 8-15.	**VLAN > VLAN**
Voice VLAN (VVID) configuration	–	"Configuring Voice Ports" section on page 7-14.	**VLAN > Voice VLAN**
Performance			
Configuring a port	None	Chapter 7, "Configuring the Switch Ports."	**Port > Port Settings**
Duplex mode	Auto on all 10/100 ports	"Changing the Port Speed and Duplex Mode" section on page 7-2.	**Port > Port Settings**
Speed on 10/100 ports	Auto	"Changing the Port Speed and Duplex Mode" section on page 7-2.	**Port > Port Settings**
Gigabit Ethernet flow control	Asymmetric **Note** This option is configurable only on the Gigabit ports.	"Configuring Flow Control on Gigabit Ethernet Ports" section on page 7-3.	**Port > Port Settings**
Inline power	Auto	"Configuring Inline Power on the Catalyst 3524-PWR Ports" section on page 7-17.	–

Table 4-2 Default Settings and Where to Change Them (continued)

Feature	Default Setting	Concepts and CLI Procedures	CMS Option
Flooding Control			
Storm control	Disabled	"Configuring Flooding Controls" section on page 7-4.	**Port > Flooding Control**
Flooding unknown unicast and multicast packets	Enabled	"Blocking Flooded Traffic on a Port" section on page 7-5.	**Port > Flooding Control**
Cisco Group Management Protocol (CGMP)	Enabled	"Configuring CGMP" section on page 6-20.	**Device > CGMP**
Multicast VLAN Registration (MVR)	Disabled	"Configuring MVR" section on page 6-27.	–
Internet Group Management Protocol (IGMP) filtering	Disabled	"Configuring IGMP Filtering" section on page 6-23.	–
Network Port	Disabled	"Enabling a Network Port" section on page 7-6.	–
Network Redundancy			
Hot Standby Router Protocol	Disabled	"Creating a Cluster Standby Group" section on page 5-21.	**Cluster > Standby Command Switches**[2]
Spanning Tree Protocol	Enabled	"Configuring STP" section on page 6-33.	**Device > STP**
Unidirectional link detection	Disabled	"Configuring UniDirectional Link Detection" section on page 7-7.	–
Port grouping	None assigned	"Creating EtherChannel Port Groups" section on page 7-8.	**Port > EtherChannels**
Diagnostics			
Displaying statistics, graphs, and reports	Enabled	"Verifying a Switch Cluster" section on page 5-23.	**Reports**
Switch Port Analyzer (SPAN) port monitoring	Disabled	"Enabling SPAN" section on page 7-13.	**Port > SPAN**
Console, buffer, and file logging	Disabled	– Documentation set for Cisco IOS Release 12.0 on Cisco.com.	–
Remote monitoring (RMON)	Disabled	"SNMP Network Management Platforms" section on page 4-5. Documentation set for Cisco IOS Release 12.0 on Cisco.com.	–

Table 4-2 Default Settings and Where to Change Them (continued)

Feature	Default Setting	Concepts and CLI Procedures	CMS Option
Security			
Password	None	"Passwords" section on page 5-14 and "Assigning Passwords and Privilege Levels" section on page 6-11. Refer to the latest switch release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm).	–
Addressing security	Disabled	"Managing the MAC Address Tables" section on page 6-15.	**Administration >MAC Addresses**
Trap manager	0.0.0.0	"Adding Trap Managers" section on page 6-49.	**Administration > SNMP**
Community strings	public	"SNMP Community Strings" section on page 5-14 and "Entering Community Strings" section on page 6-49. Documentation set for Cisco IOS Release 12.0 on Cisco.com.	**Administration > SNMP**
Port security	Disabled	"Enabling Port Security" section on page 7-11.	**Port > Port Security**
Protected port	Disabled	"Configuring Protected Ports" section on page 7-10.	**Port > Protected Port**
Terminal Access Controller Access Control System Plus (TACACS+)	Disabled	"Configuring TACACS+" section on page 6-51.	–

1. Available only from a Device Manager session on a command-capable switch, which is not a cluster member.
2. Available only from a cluster management session.

Clustering Switches

This chapter provides these topics to help you get started with switch clustering:

- Understanding Switch Clusters, page 5-2
- Planning a Switch Cluster, page 5-4
- Creating a Switch Cluster, page 5-17
- Using the CLI to Manage Switch Clusters, page 5-24
- Using SNMP to Manage Switch Clusters, page 5-25

Configuring switch clusters is more easily done from the Cluster Management Suite (CMS) web-based interface than through the command-line interface (CLI). Therefore, information in this chapter focuses on using CMS to create a cluster. See Chapter 2, "Getting Started with CMS," for additional information about switch clusters and the clustering options. For complete procedures on using CMS to configure switch clusters, refer to the online help.

For the CLI cluster commands, refer to the switch command reference.

Refer to the release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm) for the list of Catalyst switches eligible for switch clustering, including which ones can be command switches and which ones can only be member switches, and for the required software versions and browser and Java plug-in configurations.

Note This chapter focuses on Catalyst 2900 XL and Catalyst 3500 XL switch clusters. It also includes guidelines and limitations for clusters mixed with other cluster-capable Catalyst switches, but it does not provide complete descriptions of the cluster features for these other switches. For complete cluster information for a specific Catalyst platform, refer to the software configuration guide for that switch.

Understanding Switch Clusters

A switch cluster is a group of connected Catalyst switches that are managed as a single entity. In a switch cluster, 1 switch must be the *command switch* and up to 15 switches can be *member switches*. The total number of switches in a cluster cannot exceed 16 switches. The command switch is the single point of access used to configure, manage, and monitor the member switches. Cluster members can belong to only one cluster at a time.

The benefits of clustering switches include:

- Management of Catalyst switches regardless of their interconnection media and their physical locations. The switches can be in the same location, or they can be distributed across a Layer 2 network. Cluster members are connected through the management VLAN of the command switch according to the connectivity guidelines described in the "Automatic Discovery of Cluster Candidates and Members" section on page 5-4.
- Command-switch redundancy if a command switch fails. One or more switches can be designated as *standby command switches* to avoid loss of contact with cluster members. A *cluster standby group* is a group of standby command switches.
- Management of a variety of Catalyst switches through a single IP address. This conserves on IP addresses, especially if you have a limited number of them. All communication with the switch cluster is through the command switch IP address.

For other clustering benefits, see the "Advantages of Using CMS and Clustering Switches" section on page 1-6.

Refer to the release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm) for the list of Catalyst switches eligible for switch clustering, including which ones can be command switches and which ones can only be member switches, and the required software versions.

Command Switch Characteristics

A Catalyst 2900 XL or Catalyst 3500 XL command switch must meet these requirements:

- It is running Cisco IOS Release 12.0(5)XP or later.
- It has an IP address.
- It has Cisco Discovery Protocol (CDP) version 2 enabled (the default).
- It is not a command or member switch of another cluster.
- It is connected to the standby command switches and member switches through its management VLAN.
- No access lists have been defined for the switch because access lists can restrict access to a switch. Access lists are not usually used in configuring the switch, except for the access class 199 that is created when a device is configured as the command switch.

Note

- We strongly recommend that the highest-end, command-capable switch in the cluster be the command switch:
- If your switch cluster has a Catalyst 3550 switch, that switch should be the command switch.
- If your switch cluster has Catalyst 2900 XL, Catalyst 2950, and Catalyst 3500 XL switches, the Catalyst 2950 should be the command switch.
- If your switch cluster has Catalyst 1900, Catalyst 2820, Catalyst 2900 XL, and Catalyst 3500 XL switches, either the Catalyst 2900 XL or Catalyst 3500 XL should be the command switch.

Standby Command Switch Characteristics

A Catalyst 2900 XL or Catalyst 3500 XL standby command switch must meet these requirements:

- It is running 12.0(5)XP or later.
- It has an IP address.
- It has CDP version 2 enabled.
- It is connected to the command switch through the command-switch management VLAN.
- It is redundantly connected to the cluster so that connectivity to member switches is maintained.
- It is not a command or member switch of another cluster.

Note

- When the command switch is a Catalyst 3550 switch, all standby command switches must be Catalyst 3550 switches or Catalyst 2950 switches running Cisco IOS Release 12.1(6)EA2 or later.
- When the command switch is a Catalyst 2950 switch running Cisco IOS Release 12.1(6)EA2 or later, all standby command switches must be Catalyst 2950 switches running Cisco IOS Release 12.1(6)EA2 or later.
- When the Catalyst 2950 command switch is running Cisco IOS Release 12.0(5)WC2 or earlier, the standby command switches can be these switches also running Cisco IOS Release 12.0(5)WC2 or earlier: Catalyst 2900 XL, Catalyst 2950, and Catalyst 3500 XL switches.

Candidate and Member Switches Characteristics

Candidate switches are cluster-capable switches that have not yet been added to a cluster. Member switches are switches that have actually been added to a switch cluster. Although not required, a candidate or member switch can have its own IP address and password (for related considerations, see the "IP Addresses" section on page 5-13 and "Passwords" section on page 5-14).

To join a cluster, a candidate switch must meet these requirements:

- It is running cluster-capable software.
- It has CDP version 2 enabled.
- It is not a command or member switch of another cluster.
- It is connected to the command switch through the command-switch management VLAN.

Planning a Switch Cluster

Anticipating conflicts and compatibility issues is a high priority when you manage several switches through a cluster. This section describes these guidelines, requirements, and caveats that you should understand before you create the cluster:

- Automatic Discovery of Cluster Candidates and Members, page 5-4
- HSRP and Standby Command Switches, page 5-10
- IP Addresses, page 5-13
- Host Names, page 5-14
- Passwords, page 5-14
- SNMP Community Strings, page 5-14
- TACACS+, page 5-15
- Access Modes in CMS, page 5-15
- Management VLAN, page 5-16
- Network Port, page 5-16
- NAT Commands, page 5-17
- LRE Profiles, page 5-17
- Availability of Switch-Specific Features in Switch Clusters, page 5-17

Refer to the release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm) for the list of Catalyst switches eligible for switch clustering, including which ones can be command switches and which ones can only be member switches, and for the required software versions and browser and Java plug-in configurations.

Automatic Discovery of Cluster Candidates and Members

The command switch uses Cisco Discovery Protocol (CDP) to discover member switches, candidate switches, neighboring switch clusters, and edge devices in star or cascaded topologies.

Note Do not disable CDP on the command switch, on cluster members, or on any cluster-capable switches that you might want a command switch to discover. For more information about CDP, see the "Configuring CDP" section on page 6-13.

Following these connectivity guidelines ensures automatic discovery of the switch cluster, cluster candidates, connected switch clusters, and neighboring edge devices:

- Discovery through CDP Hops, page 5-5
- Discovery through Non-CDP-Capable and Noncluster-Capable Devices, page 5-6
- Discovery through Different Management VLANs, page 5-8
- Discovery through the Same Management VLAN, page 5-7
- Discovery of Newly Installed Switches, page 5-9

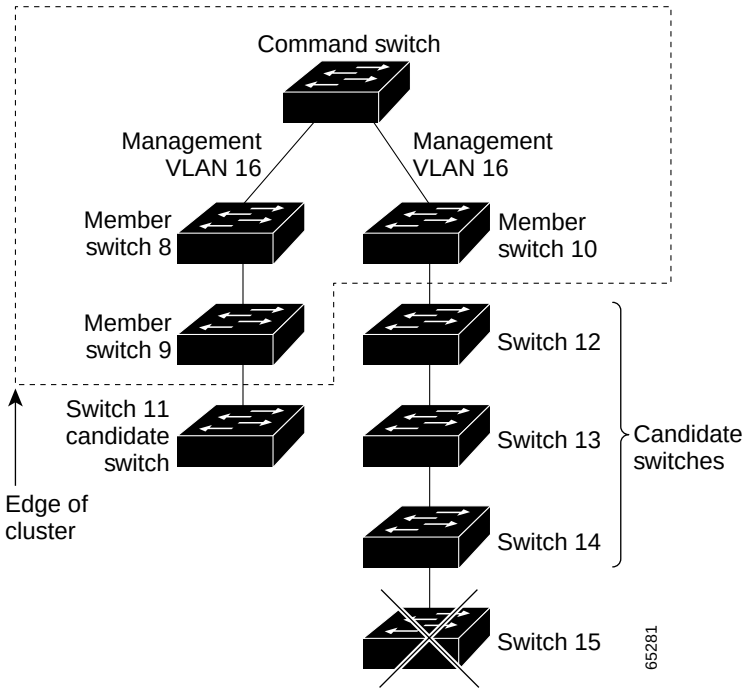
Discovery through CDP Hops

By using CDP, a command switch can discover switches up to seven CDP hops away (the default is three hops) from the edge of the cluster. The edge of the cluster is where the last member switches are connected to the cluster (for example, the command switch and member switches 8, 9, and 10 in Figure 5-1 are at the edge of the cluster).

You can set the number of hops the command switch searches for candidate and member switches by selecting **Cluster > Hop Count**. When new candidate switches are added to the network, the command switch discovers them and adds them to the list of candidate switches.

Figure 5-1 shows a switch cluster with candidate switches. The command switch has ports assigned to management VLAN 16. The CDP hop count is three. The command switch discovers switches 11, 12, 13, and 14 because they are within 3 hops from the edge of the cluster. It does not discover switch 15 because it is 4 hops from the edge of the cluster.

Figure 5-1 Discovery through CDP Hops

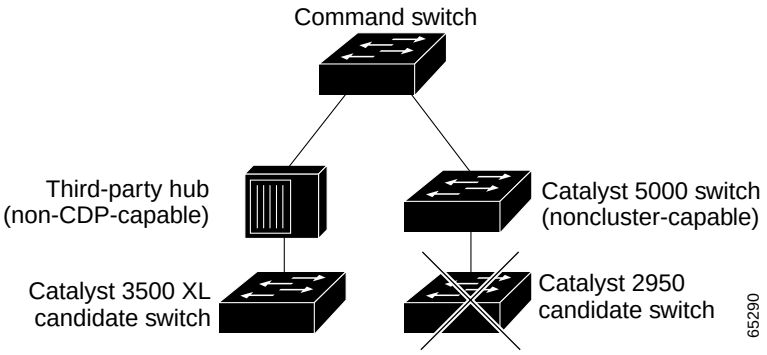


Discovery through Non-CDP-Capable and Noncluster-Capable Devices

If a command switch is connected to a *non-CDP-capable third-party hub* (such as a non-Cisco hub), it can discover cluster-enabled devices connected to that third-party hub. However, if the command switch is connected to a *noncluster-capable Cisco device*, it cannot discover a cluster-enabled device connected beyond the noncluster-capable Cisco device.

Figure 5-2 shows that the command switch discovers the Catalyst 3500 XL switch, which is connected to a third-party hub. However, the command switch does not discover the Catalyst 2950 switch that is connected to a Catalyst 5000 switch.

Figure 5-2 Discovery through Non-CDP-Capable and Noncluster-Capable Devices



Discovery through the Same Management VLAN

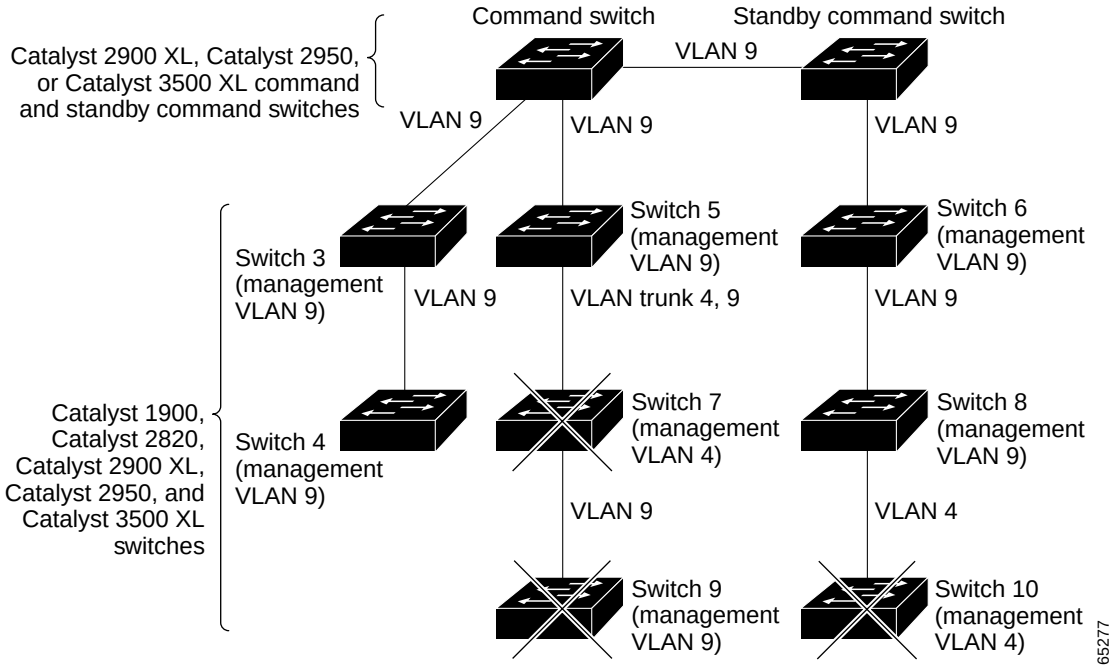
When the cluster has a Catalyst 2900 XL, Catalyst 2950, or Catalyst 3500 XL command switch, all cluster members must connect to it through the command-switch management VLAN, which is VLAN 1 by default. If the cluster members include Catalyst 3550 switches, these member switches must also be connected to the command-switch management VLAN. For information about management VLANs on these switches, see the "Management VLAN" section on page 5-16.

To avoid this limitation, assign a Catalyst 3550 switch as the command switch whenever possible. A Catalyst 3550 command switch can manage these cluster members even if they belong to different management VLANs (see the "Discovery through Different Management VLANs" section on page 5-8).

The command switch in Figure 5-3 has ports assigned to management VLAN 9. It discovers all but these switches:

- Switches 7 and 10 because their management VLAN (VLAN 4) is different from the command-switch management VLAN (VLAN 9)
- Switch 9 because automatic discovery does not extend beyond a noncandidate device, which is switch 7

Figure 5-3 Discovery through the Same Management VLAN


Command switch
Standby command switch
Catalyst 2900 XL, Catalyst 2950, or Catalyst 3500 XL command and standby command switches
VLAN 9
VLAN 9
VLAN 9
VLAN 9
Switch 5 (management VLAN 9)
Switch 6 (management VLAN 9)
Switch 3 (management VLAN 9)
VLAN 9
VLAN trunk 4, 9
VLAN 9
Catalyst 1900, Catalyst 2820, Catalyst 2900 XL, Catalyst 2950, and Catalyst 3500 XL switches
Switch 4 (management VLAN 9)
Switch 7 (management VLAN 4)
Switch 8 (management VLAN 9)
VLAN 9
VLAN 4
Switch 9 (management VLAN 9)
Switch 10 (management VLAN 4)
65277

Discovery through Different Management VLANs

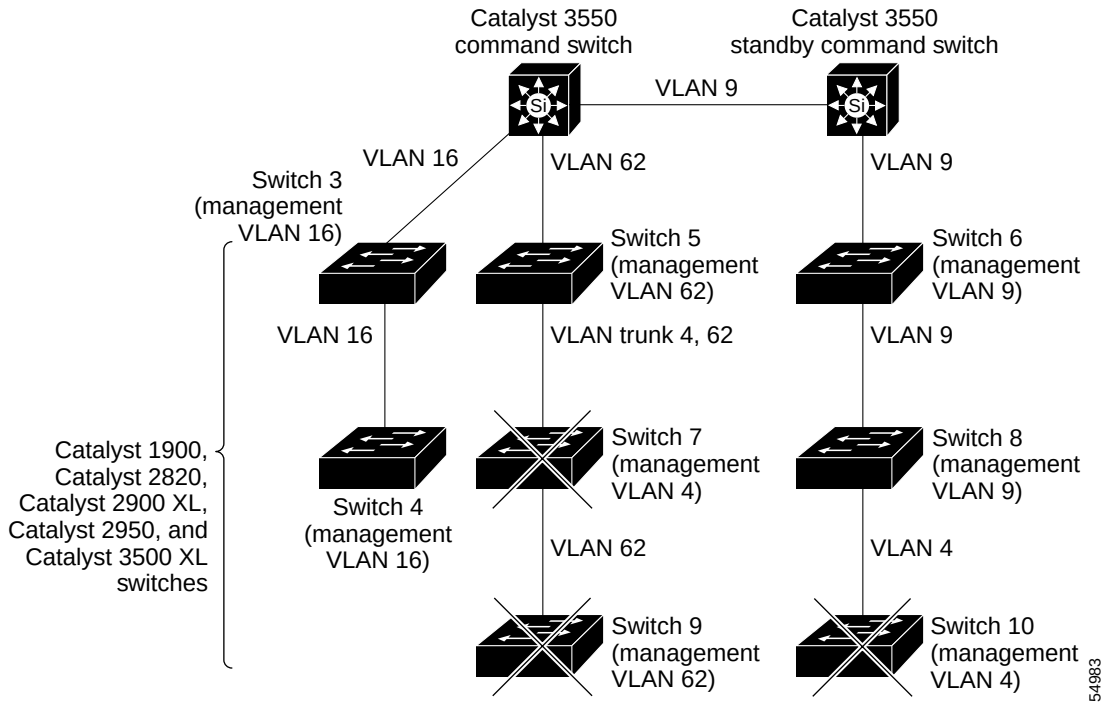
We strongly recommend that a Catalyst 3550 switch be the command switch when the cluster has Catalyst 1900, Catalyst 2820, Catalyst 2900 XL, Catalyst 2950, and Catalyst 3500 XL member switches. These member switches must connect to each other and to a Catalyst 3550 command switch through their management VLAN, which is VLAN 1 by default. When these member switches are directly connected to a Catalyst 3550 command switch, the management VLAN of these member switches can be different.

For information about discovery through the same management VLAN on these switches, see the "Discovery through the Same Management VLAN" section on page 5-7. For information about management VLANs on these switches, see the "Management VLAN" section on page 5-16.

The command switch in Figure 5-4 has ports assigned to VLANs 9, 16, and 62. It discovers all the switches in the different management VLANs except these:

- Switches 7 and 10 because their management VLAN (VLAN 4) is different from the command-switch management VLAN (VLAN 9)
- Switch 9 because automatic discovery does not extend beyond a noncandidate device, which is switch 7

Figure 5-4 Discovery through Different Management VLANs



Discovery of Newly Installed Switches

A new, out-of-the-box switch is set with the default management VLAN, VLAN 1. By default, all access ports on the new switch are assigned to management VLAN 1.

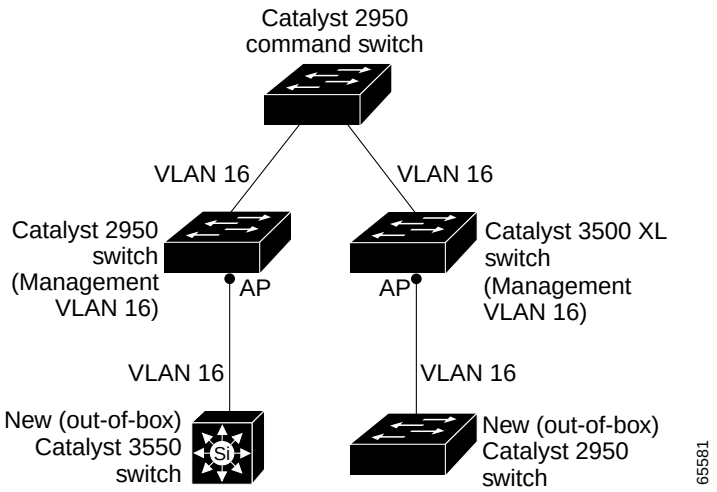
To add a new switch to a cluster, it must be connected to the cluster through an access port. When the new switch joins a cluster, its default management VLAN changes to the VLAN of the immediately upstream neighbor. The new switch also configures its access port to belong to the VLAN of the immediately upstream neighbor.

An access port (AP) carries the traffic of and belongs to the management VLAN.

For example, the command switch in Figure 5-5 belongs to management VLAN 16.

- A new Catalyst 3550 switch automatically configures the access port to belong to the immediately upstream VLAN, VLAN 16.
- A new Catalyst 2950 switch configures the access port to belong to the upstream VLAN, VLAN 16. The management VLAN of the Catalyst 2950 switch becomes VLAN 16.

Figure 5-5 Discovery of Newly Installed Switches



HSRP and Standby Command Switches

The switch supports Hot Standby Router Protocol (HSRP) so that you can configure a group of standby command switches. Because a command switch manages the forwarding of all communication and configuration information to all the member switches, we strongly recommend that you configure a cluster standby command switch to take over if the primary command switch fails.

A *cluster standby group* is a group of command-capable switches that meet the requirements described in the "Standby Command Switch Characteristics" section on page 5-3. Only one cluster standby group can be assigned per cluster.

Note

- When the command switch is a Catalyst 3550 switch, all standby command switches must be Catalyst 3550 switches or Catalyst 2950 switches running Cisco IOS Release 12.1(6)EA2 or later.
- When the command switch is a Catalyst 2950 switch running Cisco IOS Release 12.1(6)EA2 or later, all standby command switches must be Catalyst 2950 switches running Cisco IOS Release 12.1(6)EA2 or later.
- When the Catalyst 2950 command switch is running Cisco IOS Release 12.0(5)WC2 or earlier, the standby command switches can be these switches also running Cisco IOS Release 12.0(5)WC2 or earlier: Catalyst 2900 XL, Catalyst 2950, andCatalyst 3500 XL switches.

Note The cluster standby group is an HSRP group. Disabling HSRP disables the cluster standby group.

Note The switches in the cluster standby group are ranked according to HSRP priorities. The switch with the highest priority in the group is the *active command switch* (AC). The switch with the next highest priority is the *standby command switch* (SC). The other switches in the cluster standby group are the *passive command switches* (PC). If the active command switch and the standby command switch become disabled *at the same time*, the passive command switch with the highest priority becomes the active command switch. For the limitations to automatic discovery, see the "Automatic Recovery of Cluster Configuration" section on page 5-11. For information about changing HSRP priority values, refer to the **standby priority** interface configuration mode command in the Cisco IOS Release 12.0 documentation set. The HSRP standby hold time interval should be greater than or equal to 3 times the hello time interval. The default HSRP standby hold time interval is 10 seconds. The default HSRP standby hello time interval is 3 seconds. For more information about the standby hold time and hello time intervals, refer to the Cisco IOS Release 12.0 documentation set on Cisco.com.

These connectivity guidelines ensure automatic discovery of the switch cluster, cluster candidates, connected switch clusters, and neighboring edge devices. These topics also provide more detail about standby command switches:

- "Virtual IP Addresses" section on page 5-11
- "Automatic Recovery of Cluster Configuration" section on page 5-11
- "Considerations for Cluster Standby Groups" section on page 5-12

Virtual IP Addresses

You need to assign a unique virtual IP address and group number and name to the cluster standby group. This information must be configured on the management VLAN on the active command switch. The active command switch receives traffic destined for the virtual IP address. To manage the cluster, you must access the active command switch through the virtual IP address, not through the command-switch IP address. This is in case the IP address of the active command switch is different from the virtual IP address of the cluster standby group.

If the active command switch fails, the standby command switch assumes ownership of the virtual IP address and becomes the active command switch. The passive switches in the cluster standby group compare their assigned priorities to determine the new standby command switch. The passive standby switch with the highest priority then becomes the standby command switch. When the previously active command switch becomes active again, it resumes its role as the active command switch, and the current active command switch becomes the standby command switch again. For more information about IP address in switch clusters, see the "IP Addresses" section on page 5-13.

Automatic Recovery of Cluster Configuration

The active command switch continually forwards cluster-configuration information (but not device-configuration information) to the standby command switch. This ensures that the standby command switch can take over the cluster immediately after the active command switch fails.

Automatic discovery has these limitations:

- This limitation applies only to clusters that have Catalyst 2950 and Catalyst 3550 command and standby command switches: If the active command switch and standby command switch become disabled *at the same time*, the passive command switch with the highest priority becomes the active command switch. However, because it was a passive standby command switch, the previous command switch *did not* forward cluster-configuration information to it. The active command switch only forwards cluster-configuration information to the standby command switch. You must therefore rebuild the cluster.
- This limitation applies to all clusters: If the active command switch fails and there are more than two switches in the cluster standby group, the new command switch does not discover any Catalyst 1900, Catalyst 2820, and Catalyst 2916M XL member switches. You must re-add these member switches to the cluster.
- This limitation applies to all clusters: If the active command switch fails and becomes active again, it does not discover any Catalyst 1900, Catalyst 2820, and Catalyst 2916M XL member switches. You must re-add these member switches to the cluster.

When the previously active command switch resumes its active role, it receives a copy of the latest cluster configuration from the active command switch, including members that were added while it was down. The active command switch sends a copy of the cluster configuration to the cluster standby group.

Considerations for Cluster Standby Groups

In addition to providing a virtual IP address to the cluster standby group, these requirements apply:

- When the command switch is a Catalyst 3550 switch, all standby command switches must be Catalyst 3550 switches or Catalyst 2950 switches running Cisco IOS Release 12.1(6)EA2 or later.

  When the command switch is a Catalyst 2950 switch running Cisco IOS Release 12.1(6)EA2 or later, all standby command switches must be Catalyst 2950 switches running Cisco IOS Release 12.1(6)EA2 or later.

  When the Catalyst 2950 command switch is running Cisco IOS Release 12.0(5)WC2 or earlier, the standby command switches can be these switches also running Cisco IOS Release 12.0(5)WC2 or earlier: Catalyst 2900 XL, Catalyst 2950, and Catalyst 3500 XL switches.

  We recommend that the standby command switches be of the same platform family as the command switch. For example, a cluster with a Catalyst 2900 XL or Catalyst 3500 XL command switch should have Catalyst 2900 XL or Catalyst 3500 XL standby command switches.
- Only one cluster standby group can be assigned to a cluster.
- All standby-group members must be members of the cluster.

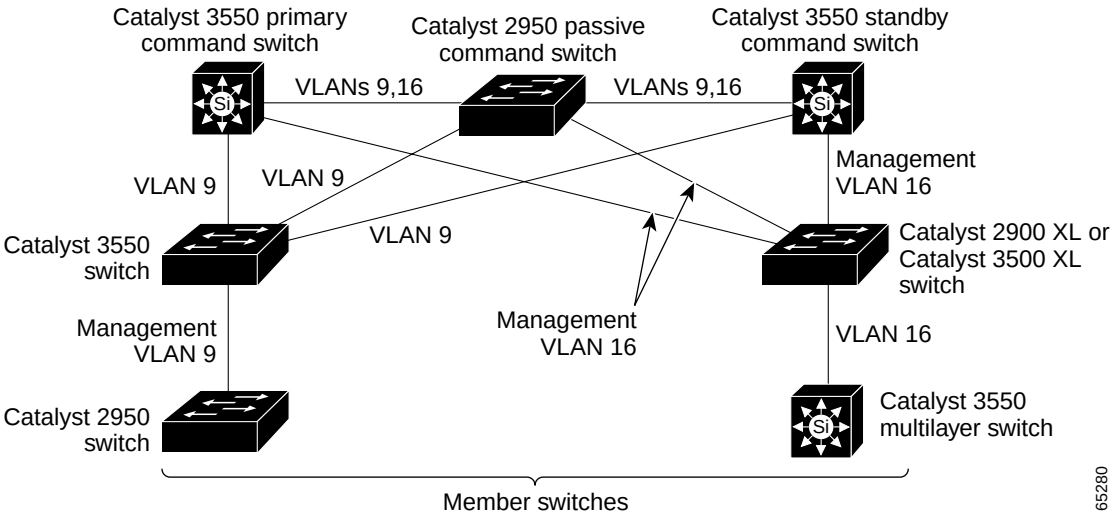
  Note There is no limit to the number of switches you can assign as standby command switches. However, the total number of switches in the cluster—which would include the active command switch, standby-group members, and member switches—cannot be more than 16.
- The active command switch must be connected through its management VLAN to each standby-group member (Figure 5-6). Each standby-group member must also be redundantly connected to each other through the management VLAN.

  Catalyst 1900, Catalyst 2820, Catalyst 2900 XL, Catalyst 2950, and Catalyst 3500 XL member switches must be connected to the cluster standby group through their management VLANs.

  For more information about VLANs in switch clusters, see these sections:

  – "Discovery through Different Management VLANs" section on page 5-8
  – "Discovery through the Same Management VLAN" section on page 5-7

Figure 5-6 VLAN Connectivity between Standby-Group Members and Cluster Members



IP Addresses

You must assign IP information to a command switch. You can access the cluster through the command-switch IP address. If you configure a cluster standby group, you must use the standby-group virtual IP address to manage the cluster from the active command switch. Using the virtual IP address ensures that you retain connectivity to the cluster if the active command switch fails and that a standby command switch becomes the active command switch.

If the active command switch fails and the standby command switch takes over, you must either use the standby-group virtual IP address to access the cluster or the IP address available on the new active command switch.

You can assign an IP address to a cluster-capable switch, but it is not necessary. A member switch is managed and communicates with other member switches through the command-switch IP address. If the member switch leaves the cluster and it does not have its own IP address, you then must assign IP information to it to manage it as a standalone switch.

Note Changing the command switch IP address ends your CMS session on the switch. Restart your CMS session by entering the new IP address in the browser **Location** field (Netscape Communicator) or **Address** field (Internet Explorer), as described in the release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm).

For more information about IP addresses, see the "Changing IP Information" section on page 6-2.

Host Names

You do not need to assign a host name to either a command switch or an eligible cluster member. However, a host name assigned to the command switch can help to more easily identify the switch cluster. The default host name for the switch is *Switch*.

If a switch joins a cluster and it does not have a host name, the command switch appends a unique member number to its own host name and assigns it sequentially as each switch joins the cluster. The number means the order in which the switch was added to the cluster. For example, a command switch named *eng-cluster* could name the fifth cluster member *eng-cluster-5*.

If a switch has a host name, it retains that name when it joins a cluster. It retains that host name even after it leaves the cluster.

If a switch received its host name from the command switch, was removed from a cluster, was then added to a new cluster, and kept the same member number (such as *5*), the old host name (such as *eng-cluster-5*) is overwritten with the host name of the command switch in the new cluster (such as *mkg-cluster-5*). If the switch member number changes in the new cluster (such as *3*), the switch retains the previous name (*eng-cluster-5*).

Passwords

It is not necessary to assign passwords to an individual switch if it will be a cluster member. When a switch joins a cluster, it inherits the command-switch password and retains it when it leaves the cluster. If no command-switch password is configured, the member switch inherits a null password. Member switches only inherit the command-switch password.

If you change the member-switch password to be different from the command-switch password and save the change, the switch is not manageable by the command switch until you change the member-switch password to match the command-switch password. Rebooting the member switch does not revert the password back to the command-switch password. We recommend that you do not change the member-switch password after it joins a cluster.

For more information about passwords, see the "Assigning Passwords and Privilege Levels" section on page 6-11.

For password considerations specific to the Catalyst 1900 and Catalyst 2820 switches, refer to the installation and configuration guides for those switches.

SNMP Community Strings

A member switch inherits the command-switch first read-only (RO) and read-write (RW) community strings with *@esN* appended to the community strings:

- *command-switch-readonly-community-string@esN*, where *N* is the member-switch number.
- *command-switch-readwrite-community-string@esN*, where *N* is the member-switch number.

If the command switch has multiple read-only or read-write community strings, only the first read-only and read-write strings are propagated to the member switch.

The switches support an unlimited number of community strings and string lengths. For more information about SNMP and community strings, see the "Configuring SNMP" section on page 6-48.

For SNMP considerations specific to the Catalyst 1900 and Catalyst 2820 switches, refer to the installation and configuration guides specific for those switches.

TACACS+

If Terminal Access Controller Access Control System Plus (TACACS+) is configured on the command switch, TACACS+ must also be configured on all member switches to access the switch cluster from CMS. For more information about TACACS+, see the "Configuring TACACS+" section on page 6-51.

Access Modes in CMS

CMS provides two levels of access to the configuration options: read-write access and read-only access. Privilege levels 0 to 15 are supported.

- Privilege level 15 provides you with read-write access to CMS.
- Privilege levels 1 to 14 provide you with read-only access to CMS. Any options in the CMS windows, menu bar, toolbar, and popup menus that change the switch or cluster configuration are not shown in read-only mode.
- Privilege level 0 denies access to CMS.

For more information about CMS access modes, see the "Access Modes in CMS" section on page 2-33.

Note

- If your cluster has these member switches running earlier software releases and if you have read-only access to these member switches, some configuration windows for those switches display incomplete information:
  - Catalyst 2900 XL or Catalyst 3500 XL member switches running Cisco IOS Release 12.0(5)WC2 or earlier
  - Catalyst 2950 member switches running Cisco IOS Release 12.0(5)WC2 or earlier
  - Catalyst 3550 member switches running Cisco IOS Release 12.1(6)EA1 or earlier

  For more information about this limitation, refer to the Catalyst 2900 XL and Catalyst 3500 XL release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm).
- These switches do not support read-only mode on CMS:
  - Catalyst 1900 and Catalyst 2820
  - Catalyst 2900 XL switches with 4-MB CPU DRAM

  In read-only mode, these switches appear as unavailable devices and cannot be configured from CMS.

Management VLAN

Communication with the switch management interfaces is through the command-switch IP address. The IP address is associated with the management VLAN, which by default is VLAN 1. To manage switches in a cluster, the command switch, member switches, and candidate switches must be connected through ports that belong to the command-switch management VLAN.

Caution You can change the management VLAN through a console connection without interrupting the console connection. However, changing the management VLAN ends your CMS session. Restart your CMS session by entering the new IP address in the browser **Location** field (Netscape Communicator) or **Address** field (Microsoft Internet Explorer), as described in the release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm).

You can change the management VLAN of a member switch (not the command switch); however, the command switch will not be able to communicate with it. In this case, you will need to manage the switch as a standalone switch.

You can globally change the management VLAN for the cluster as long as each member switch has either a trunk connection or connection to the new command-switch management VLAN. Use the **cluster management vlan** global configuration command from the command switch to change the current management VLAN of the cluster to a different management VLAN.

Note Activity synchronization is only valid if your command switch and member switches are running IOS Release 12.0(5)XU and later. Earlier releases of the software require that switches be upgraded one at a time.

Note If your cluster includes members that are running a software release earlier than Cisco IOS Release 12.0(5)XP, you cannot change the management VLAN of the cluster. If your cluster includes member switches that are running Cisco IOS Release 12.0(5)XP, those members need to have the VLAN changed before using the Management VLAN window.

If you add a new switch to an existing cluster and the cluster is using a management VLAN other than the default VLAN 1, the command switch automatically senses that the new switch has a different management VLAN and has not been configured. The command switch issues commands to change the management VLAN of the new switch to match the one in use by the cluster. This automatic change of the VLAN only occurs for new, out-of-box switches that do not have a config.text file and for which there have been no changes to the running configuration.

For more information about changing the management VLAN, see the "Changing the Management VLAN for a New Switch" section on page 8-4.

Network Port

A network port cannot link cluster members. For more information about the network port, see the "Enabling a Network Port" section on page 7-6.

NAT Commands

When a cluster is created, Network Address Translation (NAT) commands are added to the configuration file of the command switch. Do not remove these commands.

LRE Profiles

A configuration conflict occurs if a switch cluster has LRE switches using both private and public profiles. If one LRE switch in a cluster is assigned a public profile, all LRE switches in that cluster must have that same public profile. Before you add an LRE switch to a cluster, make sure that you assign it the same public profile used by other LRE switches in the cluster.

A cluster can have a mix of LRE switches using different private profiles.

For more information about the Catalyst 2900 LRE XL switches and LRE technology, refer to the Catalyst 2900 XL and Catalyst 3500 XL documentation for Cisco IOS Release 12.0(5)WC2.

Availability of Switch-Specific Features in Switch Clusters

The menu bar on the command switch displays all options available from the switch cluster. Therefore, features specific to a member switch are available from the command-switch menu bar. For example, **Device > LRE Profile** appears in the command-switch menu bar when at least one Catalyst 2900 LRE XL switch is in the cluster.

Creating a Switch Cluster

Using CMS to create a cluster is easier than using the CLI commands. This section provides this information:

- "Enabling a Command Switch" section on page 5-18
- "Adding Member Switches" section on page 5-19
- "Creating a Cluster Standby Group" section on page 5-21
- "Verifying a Switch Cluster" section on page 5-23

This section assumes you have already cabled the switches, as described in the switch hardware installation guide, and followed the guidelines described in the "Planning a Switch Cluster" section on page 5-4.

Note Refer to the release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm) for the list of Catalyst switches eligible for switch clustering, including which ones can be command switches and which ones can only be member switches, and for the required software versions and browser and Java plug-in configurations.

Enabling a Command Switch

The switch you designate to be the command switch must meet the requirements described in the "Command Switch Characteristics" section on page 5-2, "Planning a Switch Cluster" section on page 5-4, and the release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm).

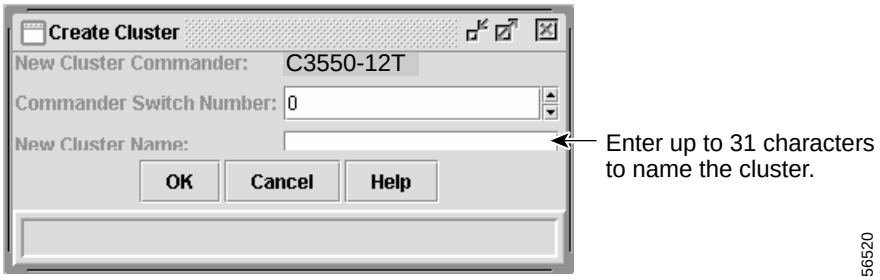
Note

- We strongly recommend that the highest-end, command-capable switch in the cluster be the command switch:
- If your switch cluster has a Catalyst 3550 switch, that switch should be the command switch.
- If your switch cluster has Catalyst 2900 XL, Catalyst 2950, and Catalyst 3500 XL switches, the Catalyst 2950 should be the command switch.
- If your switch cluster has Catalyst 1900, Catalyst 2820, Catalyst 2900 XL, and Catalyst 3500 XL switches, either the Catalyst 2900 XL or Catalyst 3500 XL should be the command switch.

You can enable a command switch, name the cluster, and assign an IP address and a password to the command switch when you run the setup program during initial switch setup. For information about using the setup program, refer to the release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm).

If you did not enable a command switch during initial switch setup, launch Device Manager from a command-capable switch, and select **Cluster > Create Cluster**. Enter a cluster number (the default is 0), and use up to 31 characters to name the cluster (Figure 5-7). Instead of using CMS to enable a command switch, you can use the **cluster enable** global configuration command.

Figure 5-7 Create Cluster Window



Adding Member Switches

As explained in the "Automatic Discovery of Cluster Candidates and Members" section on page 5-4, the command switch automatically discovers candidate switches. When you add new cluster-capable switches to the network, the command switch discovers and adds them to a list of candidate switches. To display an updated cluster candidates list from the Add to Cluster window (Figure 5-8), either relaunch CMS and redisplay this window, or follow these steps:

1. Close the Add to Cluster window.
2. Select **View** > **Refresh**.
3. Select **Cluster** > **Add to Cluster** to redisplay the Add to Cluster window.

From CMS, there are two ways to add switches to a cluster:

- Select **Cluster** > **Add to Cluster**, select a candidate switch from the list, click **Add**, and click **OK**. To add more than one candidate switch, press **Ctrl**, and make your choices, or press **Shift**, and choose the first and last switch in a range.
- Display the Topology view, right-click a candidate-switch icon, and select **Add to Cluster** (Figure 5-9). In the Topology view, candidate switches are cyan, and member switches are green. To add more than one candidate switch, press **Ctrl**, and left-click the candidates that you want to add.

Instead of using CMS to add members to the cluster, you can use the **cluster setup** privileged EXEC command or **cluster member** global configuration command from the command switch.

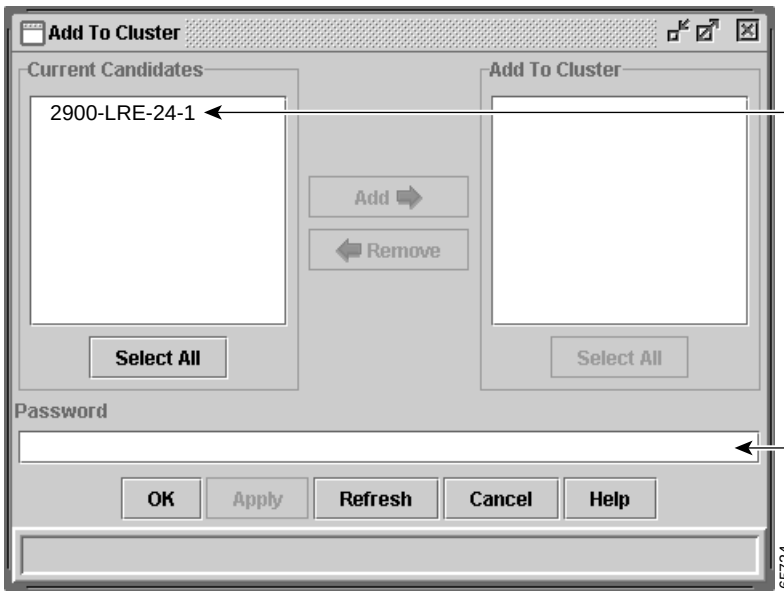
You can select one or more switches as long as the total number of switches in the cluster does not exceed 16 (this includes the command switch). When a cluster has 16 members, the **Add to Cluster** option is not available for that cluster. In this case, you must remove a member switch before adding a new one.

If a password has been configured on a candidate switch, you are prompted to enter it before you can add it to the cluster. If the candidate switch does not have a password, any entry is ignored.

If multiple candidates switches have the same password, you can select them as a group, and add them at the same time. If you incorrectly enter the password for those candidates, none of them is added to the cluster. If a candidate switch in the group has a password different from the group, only that specific candidate switch is not added to the cluster.

When a candidate switch joins a cluster, it inherits the command-switch password. For more information about setting passwords, see the "Passwords" section on page 5-14.

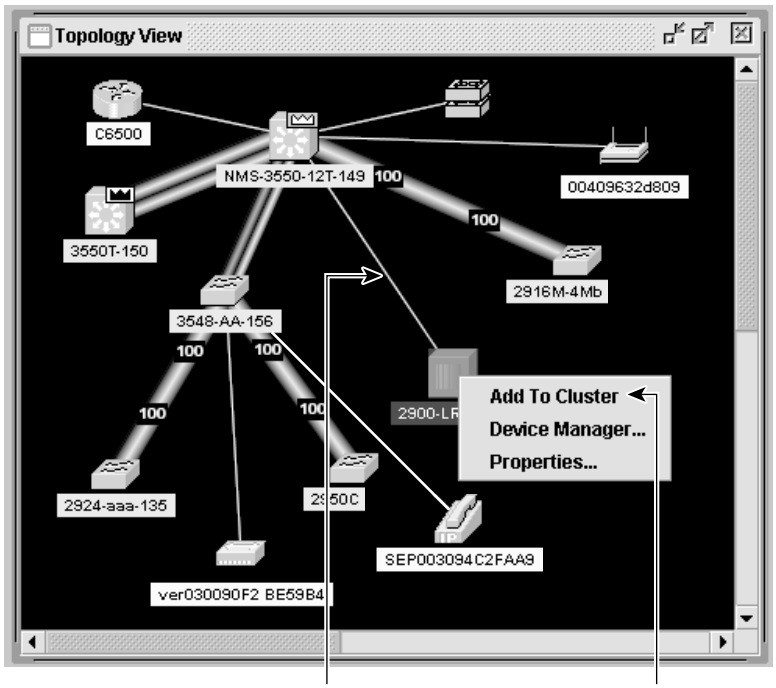
Figure 5-8 Add to Cluster Window



Select a switch, and click **Add**. Press Ctrl and left-click to select more than one switch.

Enter the password of the candidate switch. If no password exists for the switch, leave this field blank.

Figure 5-9 Using the Topology View to Add Member Switches



Thin line means a connection to a candidate switch.

Right-click a candidate switch to display the pop-up menu, and select **Add to Cluster** to add the switch to the cluster.

Creating a Cluster Standby Group

The cluster standby group members must meet the requirements described in the "Standby Command Switch Characteristics" section on page 5-3 and "HSRP and Standby Command Switches" section on page 5-10. To create a cluster standby group, select **Cluster > Standby Command Switches** (Figure 5-10).

Instead of using CMS to add switches to a standby group and to bind the standby group to a cluster, you can use the **standby ip**, **standby name**, **standby priority** interface configuration commands and the **cluster standby group** global configuration command.

Note

- When the command switch is a Catalyst 3550 switch, all standby command switches must be Catalyst 3550 switches or Catalyst 2950 switches running Cisco IOS Release 12.1(6)EA2 or later.
- When the command switch is a Catalyst 2950 switch running Cisco IOS Release 12.1(6)EA2 or later, all standby command switches must be Catalyst 2950 switches running Cisco IOS Release 12.1(6)EA2 or later.
- When the Catalyst 2950 command switch is running Cisco IOS Release 12.0(5)WC2 or earlier, the standby command switches can be these switches also running Cisco IOS Release 12.0(5)WC2 or earlier: Catalyst 2900 XL, Catalyst 2950, and Catalyst 3500 XL switches.

These abbreviations are appended to the switch host names in the Standby Command Group list to show their eligibility or status in the cluster standby group:

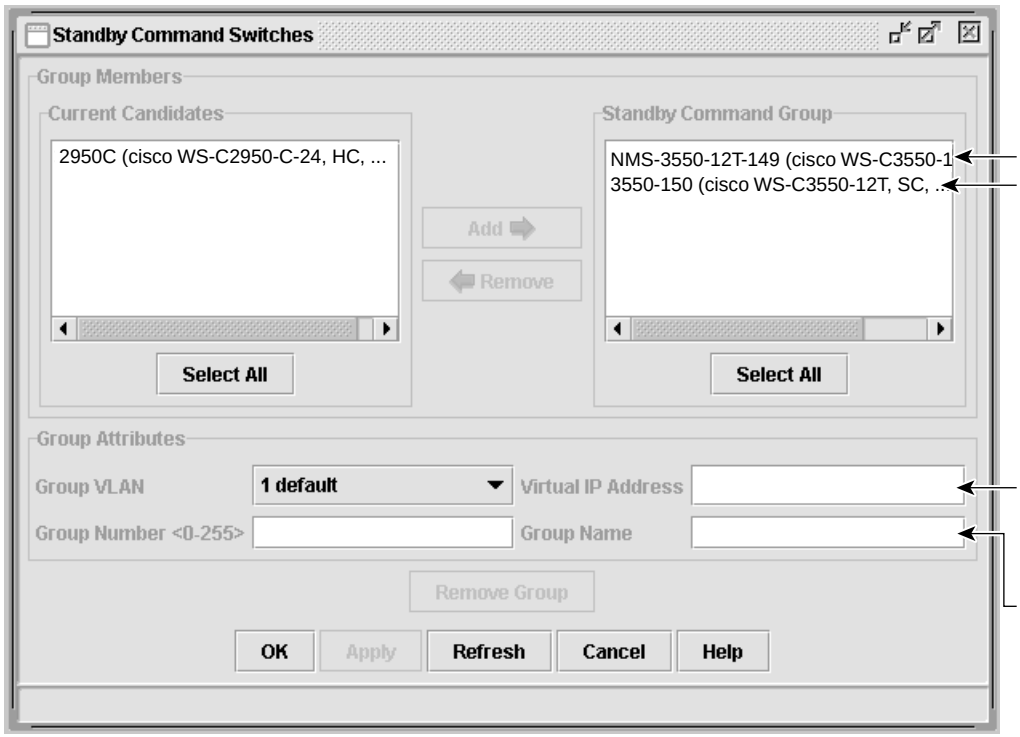
- AC—Active command switch
- SC—Standby command switch
- PC—Member of the cluster standby group but not the standby command switch
- HC—Candidate switch that can be added to the cluster standby group
- CC—Command switch when HSRP is disabled

You must enter a virtual IP address for the cluster standby group. This address must be in the same subnet as the IP addresses of the switch. The group number must be unique within the IP subnet. It can be from 0 to 255, and the default is 0. The group name can have up to 31 characters.

The Standby Command Configuration window uses the default values for the **preempt** and **name** commands that you have set by using the CLI. If you use this window to create the HSRP group, all switches in the group have the **preempt** command enabled. You must also provide a name for the group.

Note The HSRP standby hold time interval should be greater than or equal to 3 times the hello time interval. The default HSRP standby hold time interval is 10 seconds. The default HSRP standby hello time interval is 3 seconds. For more information about the standby hold time and hello time intervals, refer to the Cisco IOS Release 12.0 documentation set on Cisco.com.

Figure 5-10 Standby Command Configuration Window



Verifying a Switch Cluster

When you finish adding cluster members, follow these steps to verify the cluster:

Step 1 Enter the command switch IP address in the browser **Location** field (Netscape Communicator) or **Address** field (Microsoft Internet Explorer) to access all switches in the cluster.

Step 2 Enter the command-switch password.

Step 3 Select **View > Topology** to display the topology of the switch cluster and to view link information (Figure 2-6 on page 2-14). For complete information about the Topology view, including descriptions of the icons, links, and colors used in the Topology view, see the "Topology View" section on page 2-13.

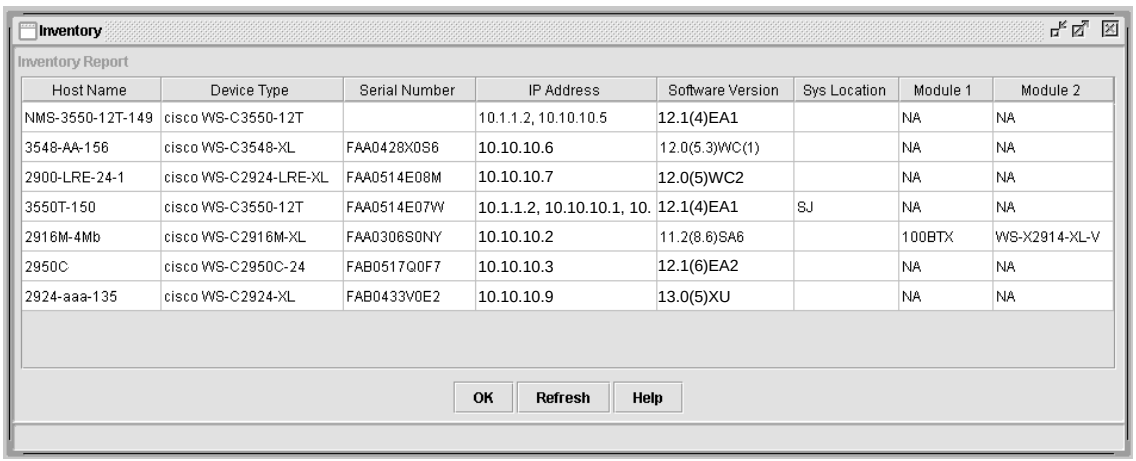
Step 4 Select **Reports > Inventory** to display an inventory of the switches in the cluster (Figure 5-11).

The summary includes information such as switch model numbers, serial numbers, software versions, IP information, and location.

You can also display port and switch statistics from **Reports > Port Statistics** and **Port > Port Settings > Runtime Status**.

Instead of using CMS to verify the cluster, you can use the **show cluster members** user EXEC command from the command switch or use the **show cluster** user EXEC command from the command switch or from a member switch.

Figure 5-11 Inventory Window


Inventory
Inventory Report
Host Name | Device Type | Serial Number | IP Address | Software Version | Sys Location | Module 1 | Module 2
NMS-3550-12T-149 | cisco WS-C3550-12T | | 10.1.1.2, 10.10.10.5 | 12.1(4)EA1 | | NA | NA
3548-AA-156 | cisco WS-C3548-XL | FAA0428X0S6 | 10.10.10.6 | 12.0(5.3)WC(1) | | NA | NA
2900-LRE-24-1 | cisco WS-C2924-LRE-XL | FAA0514E08M | 10.10.10.7 | 12.0(5)WC2 | | NA | NA
3550T-150 | cisco WS-C3550-12T | FAA0514E07W | 10.1.1.2, 10.10.10.1, 10. | 12.1(4)EA1 | SJ | NA | NA
2916M-4Mb | cisco WS-C2916M-XL | FAA0306S0NY | 10.10.10.2 | 11.2(8.6)SA6 | | 100BTX | WS-X2914-XL-V
2950C | cisco WS-C2950C-24 | FAB0517Q0F7 | 10.10.10.3 | 12.1(6)EA2 | | NA | NA
2924-aaa-135 | cisco WS-C2924-XL | FAB0433V0E2 | 10.10.10.9 | 13.0(5)XU | | NA | NA
OK
Refresh
Help
65727

If you lose connectivity with a member switch or if a command switch fails, see the "Recovery Procedures" section on page 9-11.

For more information about creating and managing clusters, refer to the online help. For information about the cluster commands, refer to the switch command reference.

Using the CLI to Manage Switch Clusters

You can configure member switches from the CLI by first logging into the command switch. Enter the **rcommand** user EXEC command and the member switch number to start a Telnet session (through a console or Telnet connection) and to access the member switch CLI. After this, the command mode changes, and the IOS commands operate as usual. Enter the **exit** privileged EXEC command on the member switch to return to the command-switch CLI.

This example shows how to log into member-switch 3 from the command-switch CLI:

```
switch# rcommand 3
```

If you do not know the member-switch number, enter the **show cluster members** privileged EXEC command on the command switch. For more information about the **rcommand** command and all other cluster commands, refer to the switch command reference.

The Telnet session accesses the member-switch CLI at the same privilege level as on the command switch. The IOS commands then operate as usual. For instructions on configuring the switch for a Telnet session, see the "Telnet Access to the CLI" section on page 4-4.

Catalyst 1900 and Catalyst 2820 CLI Considerations

If your switch cluster has Catalyst 1900 and Catalyst 2820 switches running standard edition software, the Telnet session accesses the management console (a menu-driven interface) if the command switch is at privilege level 15. If the command switch is at privilege level 1 to 14, you are prompted for the password to access the menu console.

Command-switch privilege levels map to the Catalyst 1900 and Catalyst 2820 member switches running standard and Enterprise Edition Software as follows:

- If the command-switch privilege level is 1 to 14, the member switch is accessed at privilege level 1.
- If the command-switch privilege level is 15, the member switch is accessed at privilege level 15.

Note The Catalyst 1900 and Catalyst 2820 CLI is available only on switches running Enterprise Edition Software.

For more information about the Catalyst 1900 and Catalyst 2820 switches, refer to the installation and configuration guides for those switches.

Using SNMP to Manage Switch Clusters

When you first power on the switch, SNMP is enabled if you enter the IP information by using the setup program and accept its proposed configuration. If you did not use the setup program to enter the IP information and SNMP was not enabled, you can enable it as described in the "Configuring SNMP" section on page 6-48. On Catalyst 1900 and Catalyst 2820 switches, SNMP is enabled by default.

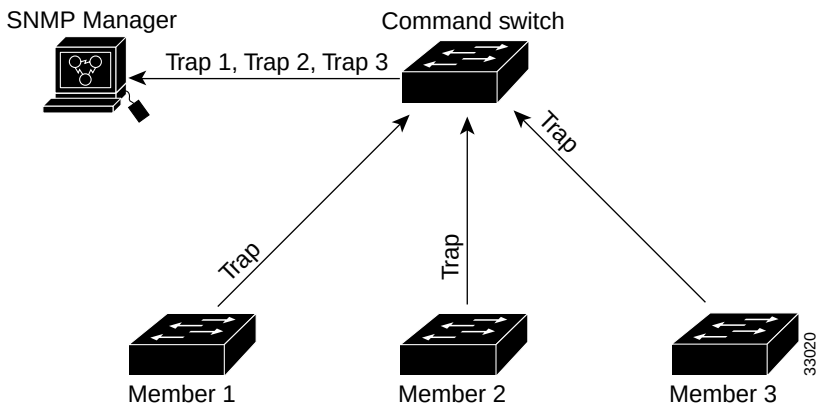
When you create a cluster, the command switch manages the exchange of messages between member switches and an SNMP application. The cluster software on the command switch appends the member switch number (*@esN*, where *N* is the switch number) to the first configured read-write and read-only community strings on the command switch and propagates them to the member switch. The command switch uses this community string to control the forwarding of gets, sets, and get-next messages between the SNMP management station and the member switches.

Note When a cluster standby group is configured, the command switch can change without your knowledge. Use the first read-write and read-only community strings to communicate with the command switch if there is a cluster standby group configured for the cluster.

If the member switch does not have an IP address, the command switch redirects traps from the member switch to the management station, as shown in Figure 5-12. If a member switch has its own IP address and community strings, the member switch can send traps directly to the management station, without going through the command switch.

If a member switch has its own IP address and community strings, they can be used in addition to the access provided by the command switch. For more information about SNMP and community strings, see the "Configuring SNMP" section on page 6-48.

Figure 5-12 SNMP Management for a Cluster



Configuring the System

This chapter provides these topics about changing switch-wide configuration settings:

- Changing IP Information, page 6-2
- Assigning Passwords and Privilege Levels, page 6-11
- Setting the System Date and Time, page 6-12
- Configuring CDP, page 6-13
- Managing the MAC Address Tables, page 6-15
- Configuring CGMP, page 6-20
- Configuring IGMP Filtering, page 6-23
- Configuring MVR, page 6-27
- Managing the ARP Table, page 6-32
- Configuring STP, page 6-33
- Configuring SNMP, page 6-48
- Configuring TACACS+, page 6-51

For information about configuring these settings from Cluster Management Suite (CMS), refer to the online help.

This switch software release is based on Cisco IOS Release 12.0. It has been enhanced to support a set of features for the Catalyst 2900 XL and Catalyst 3500 XL switches. This chapter provides procedures for using only the commands that have been created or changed for these switches. The *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference* provides complete descriptions of these commands. This guide does not provide Cisco IOS Release 12.0 commands and information already documented in the Cisco IOS Release 12.0 documentation on Cisco.com.

Changing IP Information

You can assign and change the IP information of your switch in these ways:

- Using the setup program, as described in the release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm)
- Manually assigning an IP address, as described in this section
- Using Dynamic Host Configuration Protocol (DHCP)-based autoconfiguration, as described in this section

Caution Changing the switch IP address ends any CMS, Telnet, or Simple Network Management Protocol (SNMP) session. To restart your CMS session, enter the new IP address in the browser **Location** field (Netscape Communicator) or **Address** field (Internet Explorer). To restart your CLI session through Telnet, follow the steps described in the "Accessing the CLI" section on page 3-7.

Note If you enabled the DHCP feature, the switch assumes you are using an external server for IP address allocation. While this feature is enabled, any values you manually enter (from the CMS or from the **ip address** command) are ignored.

Manually Assigning and Removing Switch IP Information

You can manually assign an IP address, mask, and default gateway to the switch. The mask identifies the bits that denote the network number in the IP address. When you use the mask to subnet a network, the mask is then referred to as a subnet mask. The broadcast address is reserved for sending messages to all hosts. The CPU sends traffic to an unknown IP address through the default gateway.

Beginning in privileged EXEC mode, follow these steps to enter the IP information:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface vlan 1**	Enter interface configuration mode, and enter the VLAN to which the IP information is assigned. VLAN 1 is the default management VLAN, but you can configure any VLAN from IDs 1 to 1001.
Step 3	**ip address** *ip_address subnet_mask*	Enter the IP address and subnet mask.
Step 4	**exit**	Return to global configuration mode.
Step 5	**ip default-gateway** *ip_address*	Enter the IP address of the default router.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show running-config**	Verify that the information was entered correctly by displaying the running configuration. If the information is incorrect, repeat the procedure.

Use this procedure to remove the IP information from a switch.

Note Using the **no ip address** command in configuration mode disables the IP protocol stack as well as removes the IP information. Cluster members without IP addresses rely on the IP protocol stack being enabled.

Beginning in privileged EXEC mode, follow these steps to remove an IP address:

	Command	Purpose
Step 1	**clear ip address vlan 1** *ip_address subnet_mask*	Remove the IP address and subnet mask.
Step 2	**end**	Return to privileged EXEC mode.
Step 3	**show running-config**	Verify that the information was removed by displaying the running configuration.

Using DHCP-Based Autoconfiguration

The Dynamic Host Configuration Protocol (DHCP) provides configuration information to Internet hosts and internetworking devices. With DHCP-based autoconfiguration, your switch (DHCP client) can be automatically configured during bootup with IP address information and a configuration file that it receives during DHCP-based autoconfiguration.

Note DHCP replaces the Bootstrap Protocol (BOOTP) feature autoconfiguration to ensure retrieval of configuration files by unicast TFTP messages. BOOTP is available in earlier software releases for this switch.

Understanding DHCP-Based Autoconfiguration

The DHCP provides configuration information to internet hosts and internetworking devices. This protocol consists of two components: one for delivering configuration parameters from a DHCP server to a device and one for allocating network addresses to devices. DHCP is built on a client-server model, where designated DHCP servers allocate network addresses and deliver configuration parameters to dynamically configured devices.

With DHCP-based autoconfiguration, your switch (DHCP client) can be automatically configured at startup with IP address information and a configuration file that it receives during DHCP-based autoconfiguration. No DHCP client-side configuration is required on your switch.

However, you need to configure the DHCP server for various lease options. You might also need to configure a TFTP server, a Domain Name System (DNS) server, and possibly a relay device if the servers are on a different LAN than your switch. A relay device forwards broadcast traffic between two directly connected LANs. A router does not forward broadcast packets, but it forwards packets based on the destination IP address in the received packet. DHCP-based autoconfiguration replaces the BOOTP client functionality on your switch.

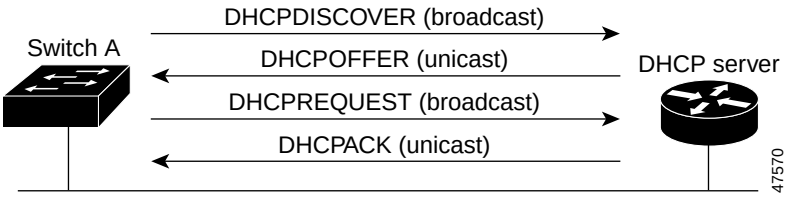
DHCP Client Request Process

When you boot your switch, the DHCP client can be invoked and automatically request configuration information from a DHCP server under these conditions:

- The configuration file is not present on the switch.
- The configuration file is present, but the IP address is not specified in it.
- The configuration file is present, the IP address is not specified in it, and the **service config** global configuration command is included. This command enables the autoloading of a configuration file from a network server.

Figure 6-1 shows the sequence of messages that are exchanged between the DHCP client and the DHCP server.

Figure 6-1 DHCP Request for IP Information from a DHCP Server



The client, Switch A, broadcasts a DHCPDISCOVER message to locate a DHCP server. The DHCP server offers configuration parameters (such as an IP address, subnet mask, gateway IP address, DNS IP address, a lease for the IP address, and so forth) to the client in a DHCPOFFER unicast message.

In a DHCPREQUEST broadcast message, the client returns a request for the offered configuration information to the DHCP server. The request is broadcast so that all other DHCP servers that received the DHCPDISCOVER broadcast message from the client can reclaim the IP addresses that they offered to the client.

The DHCP server confirms that the IP address has been allocated to the client by returning a DHCPACK unicast message to the client. With this message, the client and server are bound, and the client uses configuration information received from the server. The amount of information the switch receives depends on how you configure the DHCP server. For more information, see the "Configuring the DHCP Server" section on page 6-5.

If the configuration parameters sent to the client in the DHCPOFFER unicast message by the DHCP server are invalid (a configuration error exists), the client returns a DHCPDECLINE broadcast message to the DHCP server.

The DHCP server sends the client a DHCPNAK denial broadcast message, which means the offered configuration parameters have not been assigned, an error has occurred during the negotiation of the parameters, or the client has been slow in responding to the DHCPOFFER message (the DHCP server assigned the parameters to another client) of the DHCP server.

A DHCP client might receive offers from multiple DHCP or BOOTP servers and can accept any one of the offers; however, the client usually accepts the first offer it receives. The offer from the DHCP server is not a guarantee that the IP address will be allocated to the client; however, the server usually reserves the address until the client has had a chance to formally request the address. If the switch accepts replies from a BOOTP server and configures itself, the switch will broadcast, instead of unicast, TFTP requests to obtain the switch configuration file.

Configuring the DHCP Server

You should configure the DHCP servers with reserved leases that are bound to each switch by the switch hardware address. If the DHCP server does not support reserved leases, the switch can obtain different IP addresses and configuration files at different boot instances. You should configure the DHCP server with these lease options:

- IP address of the client (required)
- Subnet mask of the client (required)
- DNS server IP address (required)
- Router IP address (default gateway address to be used by the switch) (required)
- TFTP server name (required)
- Boot filename (the name of the configuration file that the client needs) (recommended)
- Host name (optional)

If you do not configure the DHCP server with the lease options described earlier, then it replies to client requests with only those parameters that have available values. If the IP address and subnet mask are not in the reply, the switch is not configured. If the DNS server IP address, router IP address, or TFTP server name are not found, the switch might broadcast TFTP requests. Unavailability of other lease options does not affect autoconfiguration.

Note If the configuration file on the switch does not contain the IP address, the switch obtains its address, mask, gateway IP address, and host name from DHCP. If the **service config** global configuration command is specified in the configuration file, the switch receives the configuration file through TFTP requests. If the **service config** global configuration command and the IP address are both present in the configuration file, DHCP is not used, and the switch obtains the default configuration file by broadcasting TFTP requests.

The DHCP server can be on the same or a different LAN as the switch. If it is on a different LAN, the switch must be able to access it through a relay device. The DHCP server can be running on a UNIX or Linux operating system; however, the Windows NT operating system is not supported in this release.

For more information, see the "Configuring the Relay Device" section on page 6-7. You must also set up the TFTP server with the switch configuration files; for more information, see the next section.

For CLI procedures, refer to the Cisco IOS Release 12.0 documentation on Cisco.com for additional information and CLI procedures.

Configuring the TFTP Server

The TFTP server must contain one or more configuration files in its base directory. The files can include the following:

- The configuration file named in the DHCP reply (the actual switch configuration file)
- The network-confg or the cisconet.cfg file (known as the default configuration files)
- The router-confg or the ciscortr.cfg file (These files contain commands common to all switches. Normally, if the DHCP and TFTP servers are properly configured, these files are not accessed.)

You must specify the TFTP server name in the DHCP server lease database. You must also specify the TFTP server name-to-IP-address mapping in the DNS server database.

The TFTP server can be on the same or a different LAN as the switch. If it is on a different LAN, the switch must be able to access it through a relay device or a router. For more information, see the "Configuring the Relay Device" section on page 6-7.

If the configuration filename is provided in the DHCP server reply, the configuration files for a switch can be spread over multiple TFTP servers. However, if the configuration filename is not provided, then the configuration files must reside on a single TFTP server.

For CLI procedures, refer to the Cisco IOS Release 12.0 documentation on Cisco.com for additional information and CLI procedures.

Configuring the Domain Name and the DNS

Each unique IP address can have a host name associated with it. The IOS software maintains a cache of host name-to-address mappings for use by the EXEC mode **connect**, **telnet**, and **ping** commands, and related Telnet support operations. This cache speeds the process of converting names to addresses.

IP defines a hierarchical naming scheme that allows a device to be identified by its location or domain. Domain names are pieced together with periods (.) as the delimiting characters. For example, Cisco Systems is a commercial organization that IP identifies by a *com* domain name, so its domain name is *cisco.com*. A specific device in this domain, the File Transfer Protocol (FTP) system for example, is identified as *ftp.cisco.com*.

To keep track of domain names, IP has defined the concept of a Domain Name Server (DNS), which holds a cache (or database) of names mapped to IP addresses. To map domain names to IP addresses, you must first identify the host names and then specify a name server and enable the DNS, the Internet's global naming scheme that uniquely identifies network devices.

You can specify a default domain name that the software uses to complete domain name requests. You can specify either a single domain name or a list of domain names. When you specify a domain name, any IP host name without a domain name will have that domain name appended to it before being added to the host table.

If your network devices require connectivity with devices in networks for which you do not control name assignment, you can assign device names that uniquely identify your devices within the entire internetwork. The Internet's global naming scheme, the DNS, accomplishes this task. This service is enabled by default.

The switch uses the DNS server to resolve the TFTP server name to a TFTP server IP address. You must configure the TFTP server name-to-IP address map on the DNS server. The TFTP server contains the configuration files for the switch.

You must configure the IP addresses of the DNS servers in the lease database of the DHCP server from where the DHCP replies will retrieve them. You can enter up to two DNS server IP addresses in the lease database.

The DNS server can be on the same or a different LAN as the switch. If it is on a different LAN, the switch must be able to access it through a relay device or router. For more information, see the "Configuring the Relay Device" section on page 6-7.

For CLI procedures, refer to the Cisco IOS Release 12.0 documentation on Cisco.com for additional information and CLI procedures.

Configuring the Relay Device

You need to use a relay device if the DHCP, DNS, or TFTP servers are on a different LAN than the switch. You must configure this relay device to forward received broadcast packets on an interface to the destination host. This configuration ensures that broadcasts from the DHCP client can reach the DHCP, DNS, and TFTP servers and that broadcasts from the servers can reach the DHCP client.

If the relay device is a Cisco router, you enable IP routing (**ip routing** global configuration command) and configure it with helper addresses by using the **ip helper-address** interface configuration command.

For example, in Figure 6-2, you configure the router interfaces as follows:

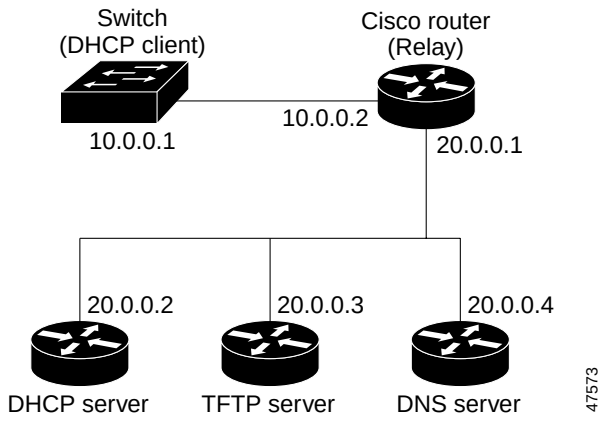
On interface 10.0.0.2:

```
router(config-if)# ip helper-address 20.0.0.2
router(config-if)# ip helper-address 20.0.0.3
router(config-if)# ip helper-address 20.0.0.4
```

On interface 20.0.0.1

```
router(config-if)# ip helper-address 10.0.0.1
```

Figure 6-2 Relay Device Used in Autoconfiguration



For CLI procedures, refer to the Cisco IOS Release 12.0 documentation on Cisco.com for additional information and CLI procedures.

Obtaining Configuration Files

Depending on the availability of the IP address and the configuration filename in the DHCP reserved lease, the switch obtains its configuration information in these ways:

- The IP address and the configuration filename is reserved for the switch and provided in the DHCP reply (one-file read method).

  The switch receives its IP address, subnet mask, and configuration filename from the DHCP server. It also receives a DNS server IP address and a TFTP server name. The switch sends a DNS request to the DNS server, specifying the TFTP server name, to obtain the TFTP server address. Then the switch sends a unicast message to the TFTP server to retrieve the named configuration file from the base directory of the server, and upon receipt, completes its boot-up process.

- Only the configuration filename is reserved for the switch. The IP address is dynamically allocated to the switch by the DHCP server (one-file read method).

  The switch follows the same configuration process described above.

- Only the IP address is reserved for the switch and provided in the DHCP reply. The configuration filename is not provided (two-file read method).

  The switch receives its IP address and subnet mask from the DHCP server. It also receives a DNS server IP address and a TFTP server name. The switch sends a DNS request to the DNS server, specifying the TFTP server name, to obtain the TFTP server address.

  The switch sends a unicast message to the TFTP server to retrieve the network-confg or cisconet.cfg default configuration file. (If the network-confg file cannot be read, the switch reads the cisconet.cfg file.)

  The default configuration file contains the host names-to-IP-address mapping for the switch. The switch fills its host table with the information in the file and obtains its host name. If the host name is not found in the file, the switch uses the host name in the DHCP reply. If the host name is not specified in the DHCP reply, the switch uses the default “Switch” as its host name.

  After obtaining its host name from the default configuration file or the DHCP reply, the switch reads the configuration file that has the same name as its host name (*hostname*-confg or *hostname*.cfg, depending on whether network-confg or cisconet.cfg was read earlier) from the TFTP server. If the cisconet.cfg file is read, the filename of the host is truncated to eight characters.

  If the switch cannot read the network-confg, cisconet.cfg, or the host-name file, it reads the router-confg file. If the switch cannot read the router-confg file, it reads the ciscortr.cfg file.

Note The switch broadcasts TFTP server requests if the TFTP server name is not obtained from the DHCP replies, if all attempts to read the configuration file through unicast transmissions fail, or if the TFTP server name cannot be resolved to an IP address.

Example Configuration

Figure 6-3 shows a sample network for retrieving IP information using DHCP-based autoconfiguration.

Figure 6-3 DHCP-Based Autoconfiguration Network Example

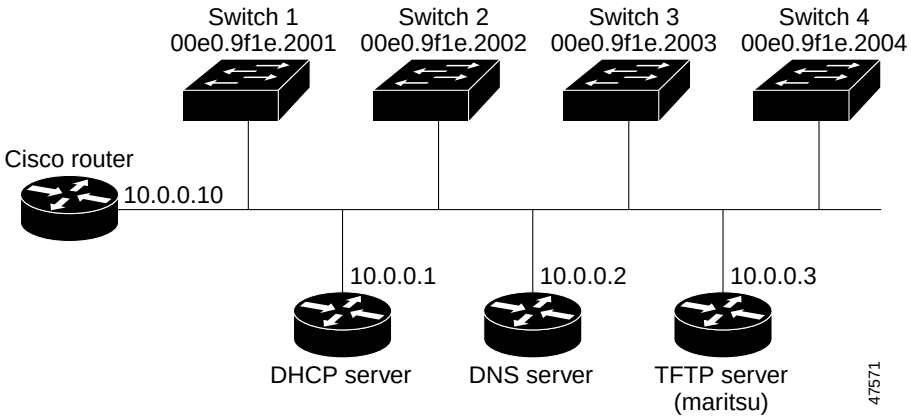


Table 6-1 shows the configuration of the reserved leases on the DHCP server.

Table 6-1 DHCP Server Configuration

	Switch-1	Switch-2	Switch-3	Switch-4
Binding key (hardware address)	00e0.9f1e.2001	00e0.9f1e.2002	00e0.9f1e.2003	00e0.9f1e.2004
IP address	10.0.0.21	10.0.0.22	10.0.0.23	10.0.0.24
Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Router address	10.0.0.10	10.0.0.10	10.0.0.10	10.0.0.10
DNS server address	10.0.0.2	10.0.0.2	10.0.0.2	10.0.0.2
TFTP server name	*maritsu* or *10.0.0.3*	*maritsu* or *10.0.0.3*	*maritsu* or *10.0.0.3*	*maritsu* or *10.0.0.3*
Boot filename (configuration file) (optional)	switch1-confg	switch2-confg	switch3-confg	switch4-confg
Host name (optional)	switch1	switch2	switch3	switch4

DNS Server Configuration

The DNS server maps the TFTP server name *maritsu* to IP address 10.0.0.3.

TFTP Server Configuration (on UNIX)

The TFTP server base directory is set to /tftpserver/work/. This directory contains the network-confg file used in the two-file read method. This file contains the host name to be assigned to the switch based on its IP address. The base directory also contains a configuration file for each switch (switch1-confg, switch2-confg, and so forth) as shown in this display:

```
prompt> cd /tftpserver/work/
prompt> ls
network-confg
switch1-confg
```

```
switch2-confg
switch3-confg
switch4-confg
prompt> cat network-confg
ip host switch1 10.0.0.21
ip host switch2 10.0.0.22
ip host switch3 10.0.0.23
ip host switch4 10.0.0.24
```

DHCP Client Configuration

No configuration file is present on Switch 1 through Switch 4.

Configuration Explanation

In Figure 6-3, Switch 1 reads its configuration file as follows:

- It obtains its IP address 10.0.0.21 from the DHCP server.
- If no configuration filename is given in the DHCP server reply, Switch 1 reads the network-confg file from the base directory of the TFTP server.
- It adds the contents of the network-confg file to its host table.
- It reads its host table by indexing its IP address 10.0.0.21 to its host name (switch1).
- It reads the configuration file that corresponds to its host name; for example, it reads switch1-confg from the TFTP server.

Switches 2 through 4 retrieve their configuration files and IP addresses in the same way.

Assigning Passwords and Privilege Levels

You can assign the password of your switch in these ways:

- Using the setup program, as described in the release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm)
- Manually assigning a password, as described in this section

Note You can change a password only by using the CLI. Your connection with the switch ends when you change the enable secret password. You will then need to reopen the session with the new password.

Because many privileged EXEC commands are used to set operating parameters, you should password-protect these commands to prevent unauthorized use. Catalyst 2900 XL and Catalyst 3500 XL switches have two commands for setting passwords:

- **enable secret** *password* (a very secure, encrypted password)
- **enable password** *password* (a less secure, unencrypted password)

You must enter one of these passwords to gain access to privileged EXEC mode. We recommend that you use the enable secret password.

Note

- When set, the enable secret password takes precedence, and the enable password serves no purpose.
- You need an enable secret password with a privilege level 15 to access CMS. You must also use this password if you configure the Terminal Access Controller Access Control System Plus (TACACS+) protocol from the CLI so that all your HTTP connections are authenticated through the TACACS+ server. The Telnet password must be an enable secret password.
- CMS provides two levels of access to the configuration options: read-write access and read-only access. Privilege levels 0 to 15 are supported.
  - Privilege level 15 provides you with read-write access to CMS.
  - Privilege levels 1 to 14 provide you with read-only access to CMS. Any options in the CMS windows, menu bar, toolbar, and popup menus that change the switch or cluster configuration are not shown in read-only mode.
  - Privilege level 0 denies access to CMS.

  For information about passwords and CMS, see the "Access Modes in CMS" section on page 2-33.
- The password of a command switch is inherited by the switches that join the switch cluster. For information about managing passwords in switch clusters, see the "Passwords" section on page 5-14.

Both types of passwords can contain from 1 to 25 uppercase and lowercase alphanumeric characters, and both can start with a number. Spaces are also valid password characters; for example, two words is a valid password. Leading spaces are ignored; trailing spaces are recognized. The password is case sensitive.

If you enter the **enable secret** command, the text is encrypted before it is written to the config.text file, and it is unreadable. If you enter the **enable password** command, the text is written as entered to the config.text file where you can read it. To remove a password, use the **no** version of the commands: **no enable secret** or **no enable password**. For CLI procedures, refer to the Cisco IOS Release 12.0 documentation on Cisco.com for additional information and CLI procedures.

You can also specify up to 15 privilege levels and define passwords for them by using the **enable password** [**level** *level*] {*password*} or the **enable secret** [**level** *level*] {*password*} command. Level 1 is EXEC-mode user privileges. If you do not specify a level, the privilege level defaults to 15 (privileged EXEC-mode privileges).

You can specify a level, set a password, and give the password only to users who need to have access at this level. Use the **privilege level** global configuration command to specify commands accessible at various levels.

If you lose or forget your enable password, see the "Recovering from a Lost or Forgotten Password" section on page 9-17.

Setting the System Date and Time

You can change the date and a 24-hour clock time setting on the switch. If you are entering the time for an American time zone, enter the three-letter abbreviation for the time zone, such as PST for Pacific standard time. If you are identifying the time zone by referring to Greenwich mean time, enter UTC (universal coordinated time). You then must enter a negative or positive number as an offset to indicate the number of time zones between the switch and Greenwich, England. Enter a negative number if the switch is west of Greenwich, England, and east of the international date line. For example, California is eight time zones west of Greenwich, so you would enter –8. Enter a positive number if the switch is east of Greenwich. You can also enter negative and positive numbers for minutes.

Configuring Daylight Saving Time

You can configure the switch to change to daylight saving time on a particular day every year, on a day that you enter, or not at all.

For CLI procedures, refer to the Cisco IOS Release 12.0 documentation on Cisco.com for additional information and CLI procedures.

Configuring the Network Time Protocol

In complex networks, it is often prudent to distribute time information from a central server. The Network Time Protocol (NTP) can distribute time information by responding to requests from clients or by broadcasting time information.

For CLI procedures, refer to the Cisco IOS Release 12.0 documentation on Cisco.com for additional information and CLI procedures.

Configuring the Switch as an NTP Client

You configure the switch as an NTP client by entering the IP addresses of up to ten NTP servers and specifying which server should be used first. You can also enter an authentication key to be used as a password when requests for time information are sent to the server.

Enabling NTP Authentication

To ensure the validity of information received from NTP servers, you can authenticate NTP messages with public-key encryption. This procedure must be coordinated with the administrator of the NTP servers: the information you enter will be matched by the servers to authenticate it.

Configuring the Switch for NTP Broadcast-Client Mode

You can configure the switch to receive NTP broadcast messages if there is an NTP broadcast server, such as a router, broadcasting time information on the network. You can also enter a value to account for any round-trip delay between the client and the NTP broadcast server.

Configuring CDP

Use the Cisco IOS CLI and Cisco Discovery Protocol (CDP) to enable CDP for the switch, set global CDP parameters, and display information about neighboring Cisco devices.

CDP enables the Cluster Management Suite to display a graphical view of the network. For example, the switch uses CDP to find cluster candidates and to maintain information about cluster members and other devices up to three cluster-enabled devices away from the command switch.

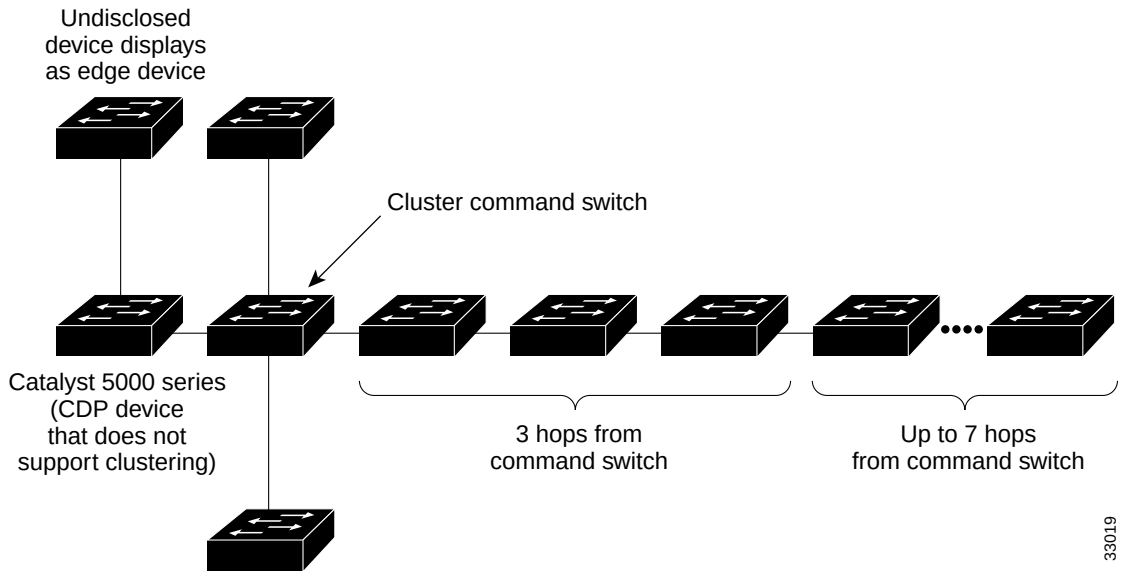
If necessary, you can configure CDP to discover switches running the Cluster Management Suite up to seven devices away from the command switch. Devices that do not run clustering software display as edge devices, and CDP cannot discover any device connected to them.

Note Creating and maintaining switch clusters is based on the regular exchange of CDP messages. Disabling CDP can interrupt cluster discovery. For more information about the role that CDP plays in clustering, see the "Automatic Discovery of Cluster Candidates and Members" section on page 5-4.

Configuring CDP for Extended Discovery

You can change the default configuration of CDP on the command switch to continue discovering devices up to seven *hops* away. Figure 6-4 shows a command switch that can discover candidates and cluster members up to seven devices away from it. Figure 6-4 also shows the command switch connected to a Catalyst 5000 series switch. Although the Catalyst 5000 supports CDP, it does not support clustering, and the command switch cannot learn about connected candidate switches connected to it, even if they are running CMS.

Figure 6-4 Discovering Cluster Candidates through CDP



Beginning in privileged EXEC mode, follow these steps to configure the number of hops that CDP uses to discover candidate switches and cluster members.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**cluster discovery hop-count** *number*	Enter the number of hops that you want CDP to search for cluster candidates and cluster members.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify the change by displaying the running configuration file. The hop count is displayed in the file.

Managing the MAC Address Tables

You can manage the MAC address tables that the switch uses to forward traffic between ports. All MAC addresses in the address tables are associated with one or more ports. These MAC tables include these types of addresses:

- Dynamic address: a source MAC address that the switch learns and then drops when it is not in use.
- Secure address: a manually entered unicast address that is usually associated with a secured port. Secure addresses do not age.
- Static address: a manually entered unicast or multicast address that does not age and that is not lost when the switch resets.

The address tables list the destination MAC address and the VLAN ID, module, and port number associated with the address. Figure 6-5 shows an example list of addresses as they would appear in the dynamic, secure, or static address table. Table 6-2 shows the maximum number of MAC addresses supported on the Catalyst 2900 XL and Catalyst 3500 XL switches.

Figure 6-5 Contents of the Address Table

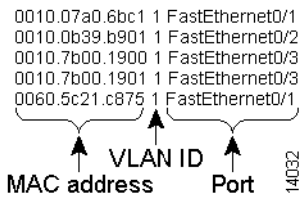


Table 6-2 Maximum Number of MAC Addresses Supported

Switch	Maximum Number of MAC Address Supported
Catalyst 2924 XL, 2924C XL, and 2912 XL switches	2048
Catalyst 2924M XL and 2912MF XL switches	8192
Catalyst 2900 LRE XL switches	8192
Catalyst 3500 XL switches	8192

MAC Addresses and VLANs

All addresses are associated with a VLAN. An address can exist in more than one VLAN and have different destinations in each. Multicast addresses, for example, could be forwarded to port 1 in VLAN 1 and ports 9, 10, and 11 in VLAN 5.

Each VLAN maintains its own logical address table. A known address in one VLAN is unknown in another until it is learned or statically associated with a port in the other VLAN. An address can be secure in one VLAN and dynamic in another. Addresses that are statically entered in one VLAN must be static addresses in all other VLANs.

Changing the Address Aging Time

Dynamic addresses are source MAC addresses that the switch learns and then drops when they are not in use. The aging time parameter defines how long the switch retains unseen addresses in the table. This parameter applies to all VLANs.

Setting too short an aging time can cause addresses to be prematurely removed from the table. Then when the switch receives a packet for an unknown destination, it floods the packet to all ports in the same VLAN as the receiving port. This unnecessary flooding can impact performance. Setting too long an aging time can cause the address table to be filled with unused addresses; it can cause delays in establishing connectivity when a workstation is moved to a new port.

Beginning in privileged EXEC mode, follow these steps to configure the dynamic address table aging time.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**mac-address-table aging-time** *seconds*	Enter the number of seconds that dynamic addresses are to be retained in the address table. You can enter a number from 10 to 1000000.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show mac-address-table aging-time**	Verify your entry.

Removing Dynamic Address Entries

Beginning in privileged EXEC mode, follow these steps to remove a dynamic address entry:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no mac-address-table dynamic** *hw-addr*	Enter the MAC address to be removed from dynamic MAC address table.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show mac-address-table**	Verify your entry.

You can remove all dynamic entries by using the **clear mac-address-table dynamic** command in privileged EXEC mode.

MAC Address Notification

MAC address notification enables you to track users coming to and going from your network. Whenever a new MAC address is learned or an old MAC address is removed from the switch, an SNMP notification (trap) is generated. If you have many users coming and going from the network, you can set a trap interval time so that traps can be bundled together and sent at regular intervals.

The MAC notification history table stores the MAC address activity for each hardware port for which the trap is enabled. MAC address notifications are generated for dynamic and secure MAC addresses. Events are not generated for self addresses, multicast addresses, or other static addresses.

Beginning in privileged EXEC mode, follow these steps to enable the MAC address notification feature:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**SNMP-server enable traps mac-notification**	Enable SNMP notification of MAC address additions and deletions.
Step 3	**mac-address-table notification**	Enable the MAC address notification feature
Step 4	**mac-address-table notification interval** *seconds*	(Optional) For **interval** *value*, specify the notification trap interval in seconds between each set of traps that are generated to the network management station (NMS). The range is 0 to 2147483647 seconds. The default is 1 second. The switch sends the notification trap to the NMS after the interval setting has expired.
Step 5	**mac-address-table notification history-size** *value*	(Optional) For **history-size** *value*, specify the maximum number of entries in the MAC notification history table. The range is 0 to 500. The default is 1 entry. **Note** The **interval** *seconds* and **history-size** *value* keywords must be entered as separate commands.
Step 6	**interface** *interface-id*	Enter interface configuration mode for the port you want to configure.
Step 7	**SNMP trap mac-notification** [**added** | **removed**]	Enable or disable MAC address traps on the port.
Step 8	**end**	Return to PRIV EXEC mode.
Step 9	**show mac-address-table notification** or **show running-config**	(Optional) Verify your settings.
Step 10	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable the switch from sending MAC address notification traps, use the **no snmp-server enable traps mac-notification** global configuration command. To disable the MAC address notification traps on a specific interface, use the **no snmp trap mac-notification** interface configuration command. To disable the MAC address notification feature, use the **no mac-address-table notification** global configuration command.

This example shows how to specify 172.20.10.10 as the NMS, enable the switch to send MAC address notification traps to the NMS, enable the MAC address notification feature, set the interval time to 60 seconds, set the history-size to 100 entries, and enable traps whenever a MAC address is added on Fast Ethernet interface 0/4.

```
Switch(config)# snmp-server host 172.20.10.10
Switch(config)# snmp-server enable traps mac-notification
Switch(config)# mac-address-table notification interval 60
Switch(config)# mac-address-table notification history-size 100
Switch(config)# interface fastethernet0/4
Switch(config-if)# snmp trap mac-notification added
```

You can verify the previous commands by entering the **show mac-address-table notification** privileged EXEC command.

Adding Secure Addresses

The secure address table contains secure MAC addresses and their associated ports and VLANs. A secure address is a manually entered unicast address that is forwarded to only one port per VLAN. If you enter an address that is already assigned to another port, the switch reassigns the secure address to the new port.

You can enter a secure port address even when the port does not yet belong to a VLAN. When the port is later assigned to a VLAN, packets destined for that address are forwarded to the port.

Beginning in privileged EXEC mode, follow these steps to add a secure address:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**mac-address-table secure** *hw-addr interface* **vlan** *vlan-id*	Enter the MAC address, its associated port, and the VLAN ID.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show mac-address-table secure**	Verify your entry.

Removing Secure Addresses

Beginning in privileged EXEC mode, follow these steps to remove a secure address:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no mac-address-table secure** *hw-addr* **vlan** *vlan-id*	Enter the secure MAC address, its associated port, and the VLAN ID to be removed.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show mac-address-table secure**	Verify your entry.

You can remove all secure addresses by using the **clear mac-address-table secure** command in privileged EXEC mode.

Adding Static Addresses

A static address has these characteristics:

- It is manually entered in the address table and must be manually removed.
- It can be a unicast or multicast address.
- It does not age and is retained when the switch restarts.

You can determine how a port that receives a packet forwards it to another port for transmission. Because all ports are associated with at least one VLAN, the switch acquires the VLAN ID for the address from the ports that you select on the forwarding map.

A static address in one VLAN must be a static address in other VLANs. A packet with a static address that arrives on a VLAN where it has not been statically entered is flooded to all ports and not learned.

Static addresses are entered in the address table with an *in-port-list*, an *out-port-list*, and a VLAN ID, if needed. Packets received from the in-port list are forwarded to ports listed in the out-port-list.

Note If the in-port-list and out-port-list parameters are all access ports in a single VLAN, you can omit the VLAN ID. In this case, the switch recognizes the VLAN as that associated with the in-port VLAN. Otherwise, you must supply the VLAN ID.

Beginning in privileged EXEC mode, follow these steps to add a static address:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**mac-address-table static** *hw-addr in-port out-port-list* **vlan** *vlan-id*	Enter the MAC address, the input port, the ports to which it can be forwarded, and the VLAN ID of those ports.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show mac-address-table static**	Verify your entry.

Removing Static Addresses

Beginning in privileged EXEC mode, follow these steps to remove a static address:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no mac-address-table static** *hw-addr* **in-port** *in-port* **out-port-list** *out-port-list* **vlan** *vlan-id*	Enter the static MAC address, the input port, the ports to which it can be forwarded, and the VLAN ID to be removed.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show mac-address-table static**	Verify your entry.

You can remove all secure addresses by using the **clear mac-address-table static** command in privileged EXEC mode.

Configuring Static Addresses for EtherChannel Port Groups

Follow these rules if you are configuring a static address to forward to ports in an EtherChannel port group:

- For default source-based port groups, configure the static address to forward to *all ports* in the port group to eliminate lost packets.
- For destination-based port groups, configure the address to forward to *only one port* in the port group to avoid the transmission of duplicate packets.

Configuring CGMP

CGMP reduces the unnecessary flooding of IP multicast packets by limiting the transmission of these packets to CGMP clients that request them. The Fast Leave feature accelerates the removal of unused CGMP groups. By default, CGMP is enabled, and the Fast Leave feature is disabled.

End stations issue join messages to become part of a CGMP group and issue leave messages to leave the group. The membership of these groups is managed by the switch and by connected routers through the further exchange of CGMP messages.

CGMP groups are maintained on a per-VLAN basis: a multicast IP address packet can be forwarded to one list of ports in one VLAN and to a different list of ports in another VLAN. When a CGMP group is added, it is added on a per-VLAN, per-group basis. When a CGMP group is removed, it is only removed in a given VLAN.

Note The same multicast MAC addresses cannot belong to both CGMP and Multicast VLAN Registration (MVR) groups. CGMP does not dynamically learn addresses that are MVR group members. If you want CGMP to learn an address that is already an MVR group member, remove the address from the MVR group.

Conversely, you cannot add an address to an MVR group if it is already a CGMP group member. If you want an address that is already a CGMP group member to be an MVR group member, remove the address from the CGMP group, and then statically add it to the MVR group. For information about MVR, see the "Configuring MVR" section on page 6-27.

Enabling the Fast Leave Feature

The CGMP Fast Leave feature reduces the delay when group members leave groups. When an end station requests to leave a CGMP group, the group remains enabled for that VLAN until all members have requested to leave. With the Fast Leave feature enabled, the switch immediately verifies if there are other group members attached to its ports. If there are no other members, the switch removes the port from the group. If there are no other ports in the group, the switch sends a message to routers connected to the VLAN to delete the entire group.

The Fast Leave feature functions only if CGMP is enabled. The client must be running IGMP version 2 for the Fast Leave feature to function properly.

Beginning in privileged EXEC mode, follow these steps to enable the CGMP Fast Leave feature:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**cgmp leave-processing**	Enable CGMP and CGMP Fast Leave.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entry.

Disabling the CGMP Fast Leave Feature

Beginning in privileged EXEC mode, follow these steps to disable the CGMP Fast Leave feature:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no cgmp leave-processing**	Disable CGMP and CGMP Fast Leave.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entry.

Changing the CGMP Router Hold-Time

The router hold-time is the number of seconds the switch waits before removing (aging) a router entry and ceasing to exchange messages with the router. If it is the last router entry in a VLAN, all CGMP groups on that VLAN are removed. You can thus enter a lower router hold-time to accelerate the removal of CGMP groups.

Note You can remove router ports before the router hold-time has expired.

Beginning in privileged EXEC mode, follow these steps to change the router hold-time.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**cgmp holdtime 400**	Configure the number of seconds the switch waits before dropping a router entry.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entry.

Removing Multicast Groups

You can reduce the forwarding of IP multicast packets by removing groups from the Current Multicast Groups table. Each entry in the table consists of the VLAN, IGMP multicast address, and ports.

You can use the CLI to clear all CGMP groups, all CGMP groups in a VLAN, or all routers, their ports, and their expiration times. Beginning in privileged EXEC mode, follow these steps to remove all multicast groups.

	Command	Purpose
Step 1	**clear cgmp group**	Clear all CGMP groups on all VLANs on the switch.
Step 2	**show cgmp**	Verify your entry by displaying CGMP information.

Configuring IGMP Filtering

IGMP filtering works with the Multicast VLAN Registration (MVR) feature to allow you to configure profiles of IP multicast groups. You can then associate these profiles with filtering action.

IGMP filters are associated with each physical switch port. These filters are applied to all VLANs associated with the physical port.

When a hostor client in a VLAN sends an IGMP join message, the IGMP message is processed by the filter on the switch port. If the configured filter causes the IGMP report to be dropped, the switch port requesting the stream of IP multicast traffic cannot receive IP multicast traffic for that group. If the filtering action permits a particular IGMP report, the IGMP report is forwarded for normal processing.

The filtering actions are configured on a per-switch-port basis.

Note IGMP filtering is supported through the CLI and SNMP.

Note IGMP filtering has no relationship with the function which directs the forwarding of IP multicast traffic. For example, IGMP filtering does not apply if CGMP or MVR is used to allow for the forwarding of IP multicast traffic.

IGMP filters can be used in the video service deployment in Ethernet to the home (ETTH). The IGMP filters specify which multicast addresses are allowed to be received by the switch.

Configuring IGMP Profiles

To configure an IGMP profile, use the **ip igmp profile** global configuration command with a profile number to create an IGMP profile and enter IGMP profile configuration mode. From this mode, you can specify the parameters of the IGMP profile to be used for filtering IGMP join requests from a switch port. When you are in IGMP profile configuration mode, you can create the profile by using these commands:

- **deny**: specifies that matching addresses are denied; this is the default condition.
- **exit**: exits from IGMP profile configuration mode.
- **no**: negates a command or sets its defaults.
- **permit**: specifies that matching addresses are permitted.
- **range**: specifies a range of IP addresses for the profile. You can enter a single IP address or a range with a start and an end address.

The default is for the switch to have no IGMP profiles configured. When a profile is configured, if neither the **permit** nor **deny** keyword is included, the default is to deny access to the range of IP addresses.

Beginning in privileged EXEC mode, follow these steps to create an IGMP profile:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip igmp profile** *profile number*	Enter IGMP profile configuration mode, and assign a number to the profile you are configuring. The range is from 1 to 4294967294.
Step 3	**permit** | **deny**	(Optional) Set the action to permit or deny access to the IP multicast address. If no action is configured, the default for the profile is to deny access.
Step 4	**range** *ip multicast address*	Enter the IP multicast address or range of IP multicast addresses to which access is being controlled. If entering a range, enter the low IP multicast address, a space, and the high IP multicast address. You can use the **range** command multiple times to enter multiple addresses or ranges of addresses.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show ip igmp profile** *profile number*	Verify the profile configuration.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To delete a profile, use the **no ip igmp profile** *profile number* global configuration command.

To delete an IP multicast address or range of IP multicast addresses, use the **no range** *ip multicast address* igmp profile command.

This example shows how to create IGMP profile 22 denying access to the single IP multicast address and how to verify the configuration. Note that because the action was to deny (the default), it does not appear in the **show ip igmp profile** *profile number* privileged EXEC command output.

```
Switch # config t
Switch(config) # ip igmp profile 22
Switch(config-igmp-profile)# deny
Switch(config-igmp-profile)# range 229.9.9.0
Switch(config-igmp-profile)# end
Switch# show ip igmp profile 22
IGMP Profile 22
    range 229.9.9.0 229.9.9.0
```

Applying IGMP Filters

To control access as defined in an IGMP profile, you apply the profile to the appropriate interfaces. IGMP profiles can be applied to Layer 2 ports only. A profile can be applied to multiple interfaces, but each interface can only have one profile applied to it.

Beginning in privileged EXEC mode, follow these steps to apply an IGMP profile to a switch port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode, and enter the physical interface to configure, for example **fastethernet 0/3**. The interface must be a Layer 2 port.
Step 3	**ip igmp filter** *profile number*	Apply the specified IGMP filter profile to the interface. The profile number can be from 1 to 4294967295.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running configuration interface** *interface-id*	Verify the configuration.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To remove a filter profile from an interface, use the **no ip igmp filter** *profile number* interface configuration command.

This example shows how to apply IGMP profile 22 to an interface and verify the configuration.

```
Switch # config t
Switch(config)# interface fastethernet 0/12
Switch(config-if)# ip igmp filter 22
Switch(config-if)# end
Switch# show running-config interface fastethernet 0/12
Building configuration...

Current configuration : 124 bytes
!
interface FastEthernet0/12
 no ip address
 shutdown
 snmp trap link-status
 ip igmp filter 22
end
```

Setting the Maximum Number of IGMP Groups

You can set the maximum number of IGMP groups that a Layer 2 interface can join. Use the **no** form of this command to set the maximum back to the default, which is no limit.

Beginning in privileged EXEC mode, follow these steps to set the maximum number of IGMP groups for an interface:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode, and enter the physical interface to configure, for example **gigabitethernet0/1**. The interface must be a Layer 2 port.
Step 3	**ip igmp max-groups** *number*	Set the maximum number of IGMP groups which the interface can join. The range is from 1 to 4294967294. The default is to have no maximum set.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running configuration interface** *interface-id*	Verify the configuration.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To remove the maximum group limitation and return to the default of no maximum, use the **no ip igmp max-groups** interface configuration command.

This example shows how to limit the number of IGMP groups that an interface can join to 20.

```
Switch# config t
Switch(config)# interface fastethernet 0/12
Switch(config-if)# ip igmp max-groups 20
Switch(config-if)# end
Switch# show running-config interface fastethernet 0/12
Building configuration...

Current configuration : 124 bytes
!
interface FastEthernet0/12
 no ip address
 shutdown
 snmp trap link-status
 ip igmp max-groups 25
 ip igmp filter 22
end
```

Configuring MVR

Multicast VLAN Registration (MVR) is designed for applications using wide-scale deployment of multicast traffic (for example, broadcast of multiple television channels) across an Ethernet ring-based service provider network. MVR allows a subscriber on a port to subscribe and unsubscribe to a multicast stream on the network-wide multicast VLAN. It allows the single multicast VLAN to be shared in the network while subscribers remain in separate VLANs. This provides the ability to continuously send multicast streams in the multicast VLAN, but to isolate the streams from the subscriber VLANs for bandwidth and security reasons.

MVR assumes that subscriber ports subscribe and unsubscribe (join and leave) these multicast streams by sending out Internet Group Management Protocol (IGMP) join and leave messages. These messages can originate from an IGMP version-2-compatible set-top box with an Ethernet connection or from a PC capable of generating IGMP version-2 messages. The switch CPU identifies IP multicast streams and their associated MAC addresses in the switch forwarding table, intercepts the IGMP messages, and modifies the forwarding table to include or remove the subscriber as a receiver of the multicast stream. This forwarding behavior selectively allows traffic to cross between the two VLANs.

Because MVR does not support IGMP dynamic joins, the user or administrator must configure static multicast addresses on the router.

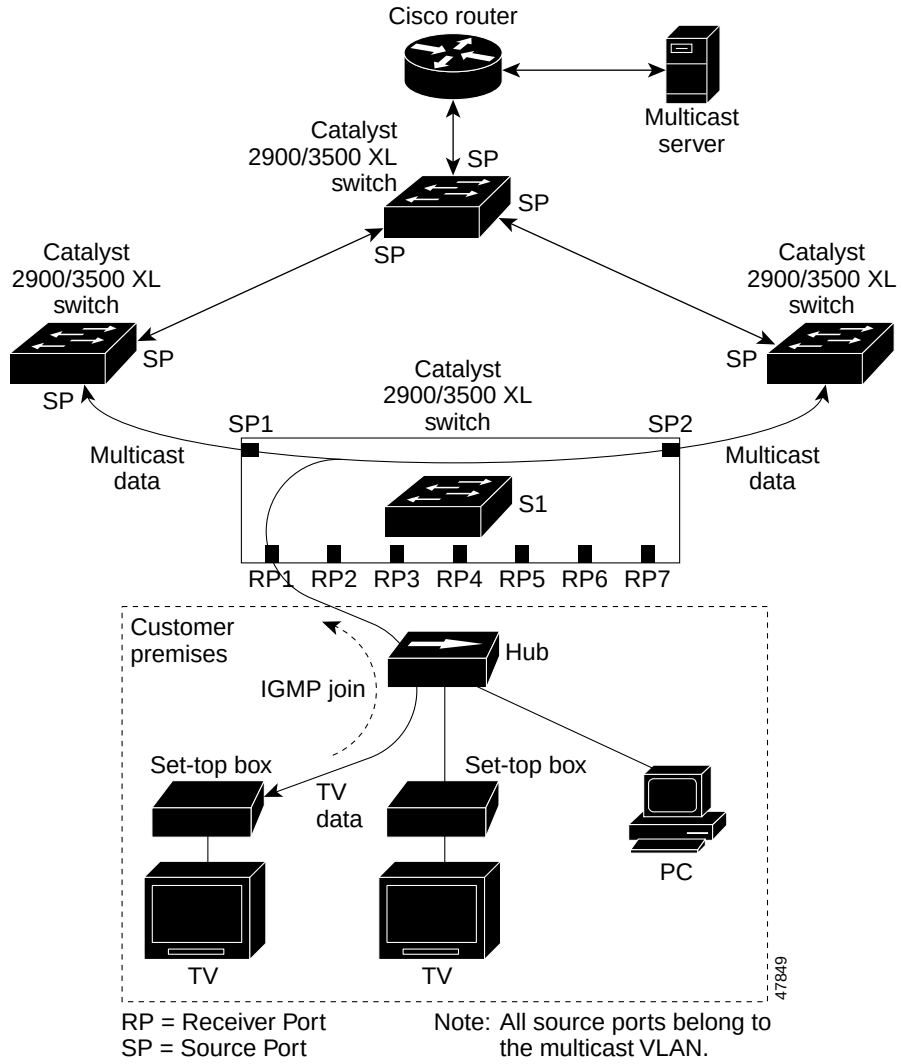
Note MVR is supported through the CLI and SNMP.

Using MVR in a Multicast Television Application

In a multicast television application, a PC or a television with a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port. (See Figure 6-6.) DHCP assigns an IP address to the set-top box or the PC. When a subscriber selects a channel, the set-top box or PC sends an IGMP report to the access layer switch (S1 switch) to join the appropriate multicast. If the IGMP report matches one of the configured multicast MAC addresses, the switch CPU modifies the hardware address table to include this receiver port and VLAN as a forwarding destination of the specified multicast stream when it is received from the multicast VLAN over the source port.

When a subscriber changes channels or turns off the television, the set-top box sends an IGMP leave message for the multicast stream. The switch CPU sends an IGMP group-specific query through the receiver port VLAN. If there is another set-top box in the VLAN still subscribing to this group, that set-top box must respond within the maximum response time. If the CPU does not receive a response, it eliminates the receiver port as a forwarding destination for this group.

Figure 6-6 Multicast VLAN Registration Example



MVR eliminates the need to duplicate television-channel multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only once around the VLAN trunk—only on the multicast VLAN. Although the IGMP leave and join messages originate with a subscriber, they appear to be initiated by a port in the multicast VLAN rather than in the VLAN to which the subscriber port is assigned. These messages dynamically register for streams of multicast traffic in the multicast VLAN on the switch. The access layer switch (S1 switch) modifies the forwarding behavior to allow the traffic to be forwarded from the multicast VLAN to the subscriber port in a different VLAN, selectively allowing traffic to cross between two VLANs.

IGMP reports are sent to the same MAC addresses as the multicast data. The S1 CPU must capture all IGMP join and leave messages from subscriber ports. Because the Catalyst 2900 and Catalyst 3500 hardware cannot distinguish IP multicast data packets from IP multicast packets carrying IGMP protocol data, all packets from subscriber ports destined for the configured multicast MAC addresses are forwarded to the switch CPU, which distinguishes IGMP packets from regular multicast traffic.

Configuration Guidelines and Limitations

Follow these guidelines when configuring MVR:

- All receiver ports on a switch must belong to the same VLAN and must not be trunk ports.
- In applications where the receiver ports represent subscribers to a service, we recommend configuring receiver ports as follows:
  - Enable protected port on all receiver ports to isolate the ports from one another.
  - Enable port blocking on all receiver ports to prevent unknown unicast and multicast packets.
- Before configuring MVR groups, configure all MVR parameters, including the multicast VLAN. If you want to change the MVR parameters after MVR groups have been configured, follow these steps:
  a. Enter the **no mvr** command to disable MVR.
  b. Enter the **mvr vlan** <*vlan-id*> command to change the multicast VLAN.
  c. The maximum number of mvr entries is determined by the switch hardware. Each MVR group represents a TV channel.
  d. Enter the **mvr** command to enable MVR. You do not need to reconfigure the MVR groups. The switch uses the MVR groups when you re-enable MVR.
- Each channel is one multicast stream destined for a unique IP multicast address.
- Make sure the router is statically configured to forward multicast traffic for the MVR groups to the switch. The router should not depend on IGMP join requests from hosts (forwarded by the switch) to forward multicast traffic to the switch.
- The receiver VLAN is the VLAN to which the first configured receiver port belongs. If the first receiver port is a dynamic port with an unassigned VLAN, it becomes an inactive receiver port and does not take part in MVR unless it is assigned to the receiver VLAN. The receiver VLAN is reset whenever there are no remaining receiver ports on the switch (active or inactive), which means that the receiver VLAN might change every time the first receiver port is configured.

MVR implementation has these limitations:

- MVR is supported on all Catalyst 3500 XL switches and on only the modular Catalyst 2900 XL switches.
- Unknown multicast packets, unknown unicast packets, and broadcast packets are leaked from the multicast VLAN to the receiver ports.
- MVR does not support IP-address aliasing and therefore requires that each IP multicast address maps to only one Layer 2 MAC address. In MVR, you cannot configure multiple IP addresses that map to the same MAC address.
- The same multicast MAC addresses cannot belong to both CGMP and MVR groups. CGMP does not dynamically learn addresses that are MVR group members. If you want CGMP to learn an address that is already an MVR group member, remove the address from the MVR group.

  Conversely, you cannot add an address to an MVR group if it is already a CGMP group member. If you want an address that is already a CGMP group member to be an MVR group member, remove the address from the CGMP group, and then statically add it to the MVR group. For information about CGMP, see the "Configuring CGMP" section on page 6-20.

Setting MVR Parameters

You do not need to set MVR parameters if you choose to use the default settings. If you do want to change the default parameters, you must do so before enabling MVR.

Beginning in privileged EXEC mode, follow these steps to configure MVR parameters:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**mvr querytime** *value*	(Optional) Define the maximum time to wait for IGMP report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a second. The default is 5 tenths or one-half second.
Step 3	**mvr vlan** *vlan-id*	(Optional) Specify the VLAN in which multicast data will be received; all source ports must belong to this VLAN. The default is VLAN 1.
Step 4	**interface** *interface*	Enter interface configuration mode, and enter the type and number of the port to configure, for example, fastethernet 0/1.
Step 5	**mvr threshold** *value*	(Optional) Define the maximum of multicast data packets received on a receiver port before it is administratively shut down. The default is 20.
Step 6	**end**	Exit configuration mode.
Step 7	**show mvr** **show mvr interface**	Verify the configuration.
Step 8	**copy running-config startup-config**	Save your configuration changes to nonvolatile RAM (NVRAM).

Configuring MVR

Beginning in privileged EXEC mode, follow these steps to configure MVR:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**mvr**	Enable MVR on the switch.
Step 3	**mvr group** *ip-address* [*count*]	Configure an IP multicast address on the switch or use the *count* parameter to configure a contiguous series of IP addresses. Any multicast data sent to this address is sent to all source ports on the switch and all receiver ports that have elected to receive data on that multicast address. Each multicast address would correspond to one television channel. **Note** Each IP address translates to a multicast 48-bit MAC address. If an IP address being configured translates (aliases) to a previously configured MAC address, the command fails.
Step 4	**interface** *interface*	Enter interface configuration mode, and enter the type and number of the port to configure, for example, fastethernet 0/1.
Step 5	**mvr type** *value*	Configure the port as either an MVR receiver port or an MVR source port. • Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by using IGMP leave and join messages. • Configure uplink ports that receive and send multicast data as source ports. All source ports on a switch belong to the single multicast VLAN.
Step 6	**mvr immediate**	(Optional) Enables the Immediate Leave feature of MVR on the port. **Note** This command applies only to receiver ports and should only be enabled on receiver ports to which a single receiver device is connected.
Step 7	**end**	Exit configuration mode.
Step 8	**show mvr** **show mvr interface** **show mvr members**	Verify the configuration.
Step 9	**copy running-config startup-config**	Save your configuration changes to NVRAM.

Managing the ARP Table

To communicate with a device (over Ethernet, for example), the software first must determine the 48-bit MAC or the local data link address of that device. The process of determining the local data link address from an IP address is called *address resolution*.

The Address Resolution Protocol (ARP) associates a host IP address with the corresponding media or MAC addresses and the VLAN ID. Taking an IP address as input, ARP determines the associated MAC address. Once a MAC address is determined, the IP-MAC address association is stored in an ARP cache for rapid retrieval. Then the IP datagram is encapsulated in a link-layer frame and sent over the network. Encapsulation of IP datagrams and ARP requests and replies on IEEE 802 networks other than Ethernet is specified by the Subnetwork Access Protocol (SNAP). By default, standard Ethernet-style ARP encapsulation (represented by the **arpa** keyword) is enabled on the IP interface.

ARP entries added manually to the table do not age and must be manually removed.

For CLI procedures, refer to the Cisco IOS Release 12.0 documentation on Cisco.com for additional information and CLI procedures.

Configuring STP

Spanning Tree Protocol (STP) provides path redundancy while preventing undesirable loops in the network. Only one active path can exist between any two stations. STP calculates the best loop-free path throughout the network.

Supported STP Instances

You create an STP instance when you assign an interface to a VLAN. The STP instance is removed when the last interface is moved to another VLAN. You can configure switch and port parameters before an STP instance is created. These parameters are applied when the STP instance is created. You can change all VLANs on a switch by using the **stp-list** parameter when you enter STP commands through the CLI. For more information, refer to the *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference*.

The Catalyst 2912 XL, Catalyst 2924 XL, and Catalyst 2924C XL support only 64 STP instances and 64 VLANs. All other Catalyst 2900 XL switches and all Catalyst 3500 XL switches support 64 STP instances and 250 VLANs.

Each VLAN is a separate STP instance. If you have already used up all available STP instances on a switch, adding another VLAN anywhere in the VLAN Trunking Protocol (VTP) domain creates a VLAN that is not running STP on that switch. For example, if 250 VLANs are defined in the VTP domain, you can enable STP on 64 of those VLANs. The remaining VLANs must operate with STP disabled.

You can disable STP on one of the VLANs where it is running, and then enable it on the VLAN where you want it to run. Use the **no spanning-tree vlan** *vlan-id* global configuration command to disable STP on a specific VLAN, and use the **spanning-tree vlan** *vlan-id* global configuration command to enable STP on the desired VLAN.

For more information about VLANs, see Chapter 8, “Configuring VLANs.”

Caution Switches that are not running spanning tree still forward Bridge Protocol Data Units (BPDUs) that they receive so that the other switches on the VLAN that have a running STP instance can break loops. Therefore, spanning tree must be running on enough switches so that it can break all the loops in the network. For example, at least one switch on each loop in the VLAN must be running spanning tree. It is not absolutely necessary to run spanning tree on all switches in the VLAN; however, if you are running STP only on a minimal set of switches, an incautious change to the network that introduces another loop into the VLAN can result in a broadcast storm.

Note If you have the default allowed list on the trunk ports of that switch, the new VLAN is carried on all trunk ports. Depending on the topology of the network, this could create a loop in the new VLAN that will not be broken, particularly if there are several adjacent switches that all have run out of STP instances. You can prevent this by setting allowed lists on the trunk ports of switches that have used up their allocation of STP instances. Setting up allowed lists is not necessary in many cases and makes it more labor-intensive to add another VLAN to the network.

Using STP to Support Redundant Connectivity

You can create a redundant backbone with STP by connecting two of the switch ports to another device or to two different devices. STP automatically disables one port but enables it if the other port is lost. If one link is high-speed and the other low-speed, the low-speed link is originally disabled. If the two link speeds are the same, the port priority and the port ID are added together, and STP disables the link with the lowest value.

You can also create redundant links between switches by using EtherChannel port groups. For more information about creating port groups, see the "Creating EtherChannel Port Groups" section on page 7-8.

Disabling STP

STP is enabled by default. Disable STP only if you are sure there are no loops in the network topology.

Caution When STP is disabled and loops are present in the topology, excessive traffic and indefinite packet duplication can severely reduce network performance.

Beginning in privileged EXEC mode, follow these steps to disable STP:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no spanning-tree vlan** *stp-list*	Disable STP on a VLAN.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show spanning-tree**	Verify your entry.

Accelerating Aging to Retain Connectivity

The default for aging dynamic addresses is 5 minutes. However, a reconfiguration of the spanning tree can cause many station locations to change. Because these stations could be unreachable for 5 minutes or more during a reconfiguration, the address-aging time is accelerated so that station addresses can be dropped from the address table and then relearned. The accelerated aging is the same as the forward-delay parameter value when STP reconfigures.

Because each VLAN is a separate instance of STP, the switch accelerates aging on a per-VLAN basis. A reconfiguration of STP on one VLAN can cause the dynamic addresses learned on that VLAN to be subject to accelerated aging. Dynamic addresses on other VLANs can be unaffected and remain subject to the aging interval entered for the switch.

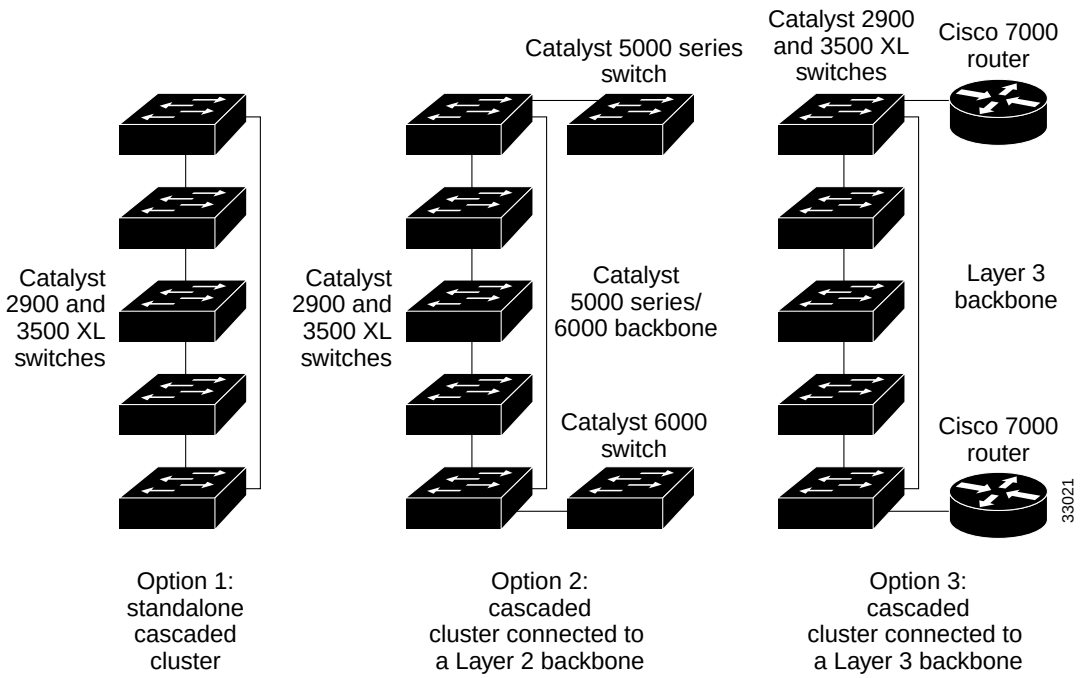
Configuring STP and UplinkFast in a Cascaded Cluster

STP uses default values that can be reduced when configuring Catalyst 2900 XL and Catalyst 3500 XL switches in cascaded configurations. If an STP root switch is part of a cluster that is one switch from a cascaded stack, you can customize STP to reconverge more quickly after a switch failure. Figure 6-7 shows modular Catalyst 2900 XL and Catalyst 3500 XL switches in three cascaded clusters that use the GigaStack GBIC. Table 6-3 shows the default STP settings and those that are acceptable for these configurations.

Table 6-3 Default and Acceptable STP Parameter Settings (in Seconds)

STP Parameter	STP Default (IEEE)	Acceptable for Option 1	Acceptable for Option 2	Acceptable for Option 3
Hello Time	2	1	1	1
Max Age	20	6	10	6
Forwarding delay	15	4	7	4

Figure 6-7 Gigabit Ethernet Clusters


Catalyst 5000 series switch
Catalyst 2900 and 3500 XL switches
Cisco 7000 router
Catalyst 2900 and 3500 XL switches
Catalyst 5000 series/ 6000 backbone
Layer 3 backbone
Catalyst 6000 switch
Cisco 7000 router
33021
Option 1: standalone cascaded cluster
Option 2: cascaded cluster connected to a Layer 2 backbone
Option 3: cascaded cluster connected to a Layer 3 backbone

Enabling UplinkFast on all cluster switches can further reduce the time it takes cluster switches to begin forwarding after a new root switch is selected.

Configuring Redundant Links By Using STP UplinkFast

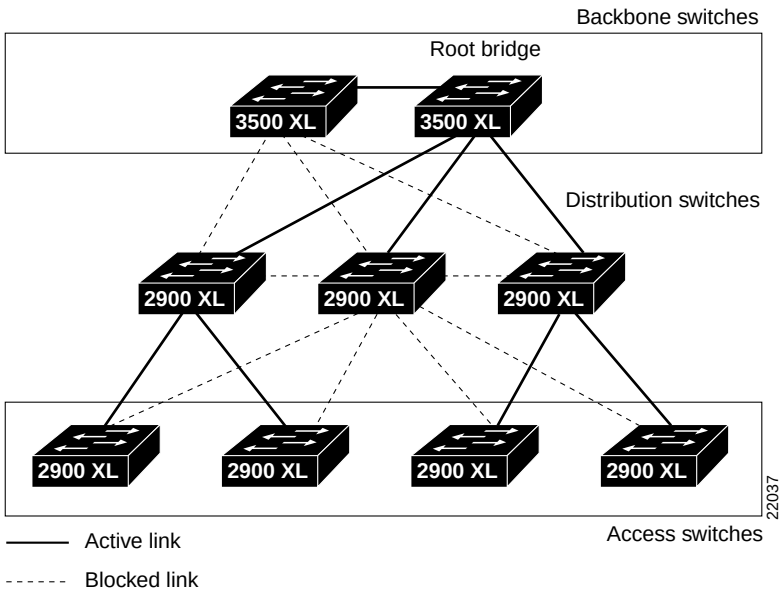
Switches in hierarchical networks can be grouped into backbone switches, distribution switches, and access switches. Figure 6-8 shows a complex network where distribution switches and access switches each have at least one redundant link that STP blocks to prevent loops.

If a switch looses connectivity, the switch begins using the alternate paths as soon as STP selects a new root port. STP UplinkFast is a Cisco enhancement that accelerates the choice of a new root port when a link or switch fails or when STP reconfigures itself. The root port transitions to the forwarding state immediately without going through the listening and learning states, as it would with normal STP procedures.

When STP reconfigures the new root port, other ports flood the network with multicast packets, one for each address that was learned on the port. You can limit these bursts of multicast traffic by reducing the max-update-rate parameter. The default for this parameter is 150 packets per second. However, if you enter zero, station-learning frames are not generated, so the STP topology converges more slowly after a loss of connectivity.

UplinkFast is most useful in edge or access switches and might not be appropriate for backbone devices.

Figure 6-8 Switches in a Hierarchical Network



Enabling STP UplinkFast

When you enable UplinkFast, it is enabled for the entire switch and cannot be enabled for individual VLANs.

Beginning in privileged EXEC mode, follow these steps to configure UplinkFast:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**spanning-tree uplinkfast max-update-rate** *pkts-per-second*	Enable UplinkFast on the switch. The range is from 0 to 1000 packets per second. The default is 150. If you set the rate to 0, station-learning frames are not generated, so the STP topology converges more slowly after a loss of connectivity.
Step 3	**exit**	Return to privileged EXEC mode.
Step 4	**show spanning-tree**	Verify your entries.

When UplinkFast is enabled, the bridge priority of all VLANs is set to 49152, and the path cost of all ports and VLAN trunks is increased by 3000. This change reduces the chance that the switch will become the root switch. When UplinkFast is disabled, the bridge priorities of all VLANs and path costs of all ports are set to default values.

Configuring Cross-Stack UplinkFast

Cross-stack UplinkFast (CSUF) provides a fast spanning-tree transition (fast convergence in less than 2 seconds under normal network conditions) across a stack of switches that use the GigaStack GBICs connected in a shared cascaded configuration (multidrop backbone). During the fast transition, an alternate redundant link on the stack of switches is placed into the forwarding state without causing temporary spanning-tree loops or loss of connectivity to the backbone. With this feature, you can have a redundant and resilient network in some configurations.

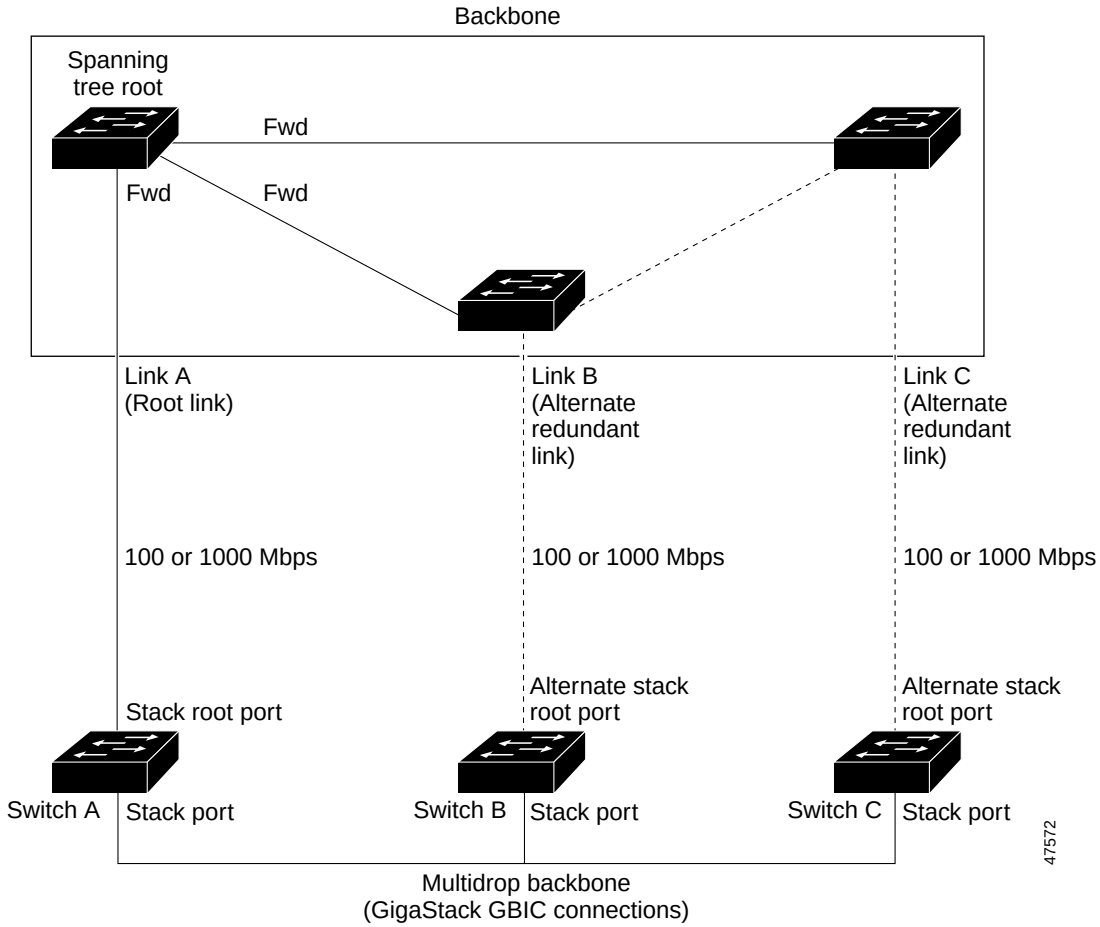
CSUF might not provide a fast transition all the time; in these cases, the normal STP transition occurs, which completes in 30 to 40 seconds. For more information, see the "Events that Cause Fast Convergence" section on page 6-39.

How CSUF Works

CSUF ensures that one link in the stack is elected as the path to the root. As shown in Figure 6-9, Switches A, B, and C are cascaded through the Gigastack GBIC to form a multidrop backbone, which communicates control and data traffic across the switches at the access layer. The switches in the stack use their stack ports to communicate with each other and to connect to the stack backbone; stack ports are always in the STP forwarding state. The stack root port on Switch A provides the path to the root of the spanning tree; the alternate stack root ports on Switches B and C can provide an alternate path to the spanning-tree root if the current stack root switch fails or its link to the spanning-tree root fails.

Link A, the root link, is in the STP forwarding state; Links B and C are alternate redundant links that are in the STP blocking state. If Switch A fails, if its stack root port fails, or if Link A fails, CSUF selects either the Switch B or Switch C alternate stack root port and puts it into the forwarding state in less than 1 second.

Figure 6-9 Cross-Stack UplinkFast Topology



CSUF implements the Stack Membership Discovery Protocol and the Fast Uplink Transition Protocol. Using the Stack Membership Discovery Protocol, all stack switches build a neighbor list of stack members through the receipt of discovery hello packets. When certain link loss or STP events occur (described in the "Events that Cause Fast Convergence" section on page 6-39), the Fast Uplink Transition Protocol uses the neighbor list to send fast-transition requests on the stack port to stack members.

The switch sending the fast-transition request needs to do a fast transition to the forwarding state of a port that it has chosen as the root port, and it must obtain an acknowledgement from each stack switch before performing the fast transition.

Each switch in the stack determines if the sending switch is a better choice than itself to be the stack root of this STP instance by comparing STP root, cost, and bridge ID. If the sending switch is the best choice as the stack root, the switch in the stack returns an acknowledgement; otherwise, it does not respond to the sending switch (drops the packet) and prevents the sending switch from receiving acknowledgements from all stack switches.

When acknowledgements are received from all stack switches, the Fast Uplink Transition Protocol on the sending switch immediately transitions its alternate stack root port to the forwarding state. If acknowledgements from all stack switches are not obtained by the sending switch, the normal STP transitions (blocking, listening, learning, forwarding) take place, and the spanning-tree topology converges at its normal rate (2 * forward-delay time + max-age time). The Fast Uplink Transition Protocol is implemented on a per-VLAN basis and affects only one STP instance at a time.

Events that Cause Fast Convergence

Depending on the network event or failure, fast convergence provided by CSUF might or might not occur.

Fast convergence (within 2 seconds under normal network conditions) occurs under these circumstances:

- The stack root port link goes down.

  If two switches in the stack have alternate paths to the root, only one of the switches performs the fast transition.
- The failed link, which connected the stack root to the STP root, comes back up.
- A network reconfiguration causes a new stack root switch to be selected.
- A network reconfiguration causes a new port on the current stack root switch to be chosen as the stack root port.

Note The fast transition might not occur if multiple events occur simultaneously. For example, if a stack member switch is powered down, and at the same time, a link connecting the stack root to the STP root comes back up, the normal STP convergence occurs.

Normal STP convergence (30 to 40 seconds) occurs under these conditions:

- The stack root switch is powered down or the software failed.
- The stack root switch, which was powered down or failed, is powered up.
- A new switch, which might become the stack root, is added to the stack.
- A switch other than the stack root is powered down or failed.
- A link fails between stack ports on the multidrop backbone.

Note The fast transition of CSUF depends on the amount of network traffic and how you connect the GigaStack GBICs across the stack switches. Because the Fast Uplink Transition Protocol only waits 2 seconds to receive acknowledgements from all stack switches, heavy network traffic might prevent the fast transition from occurring within this time frame. Instead of a fast transition, the normal STP convergence then occurs.

Limitations

These limitations apply to CSUF:

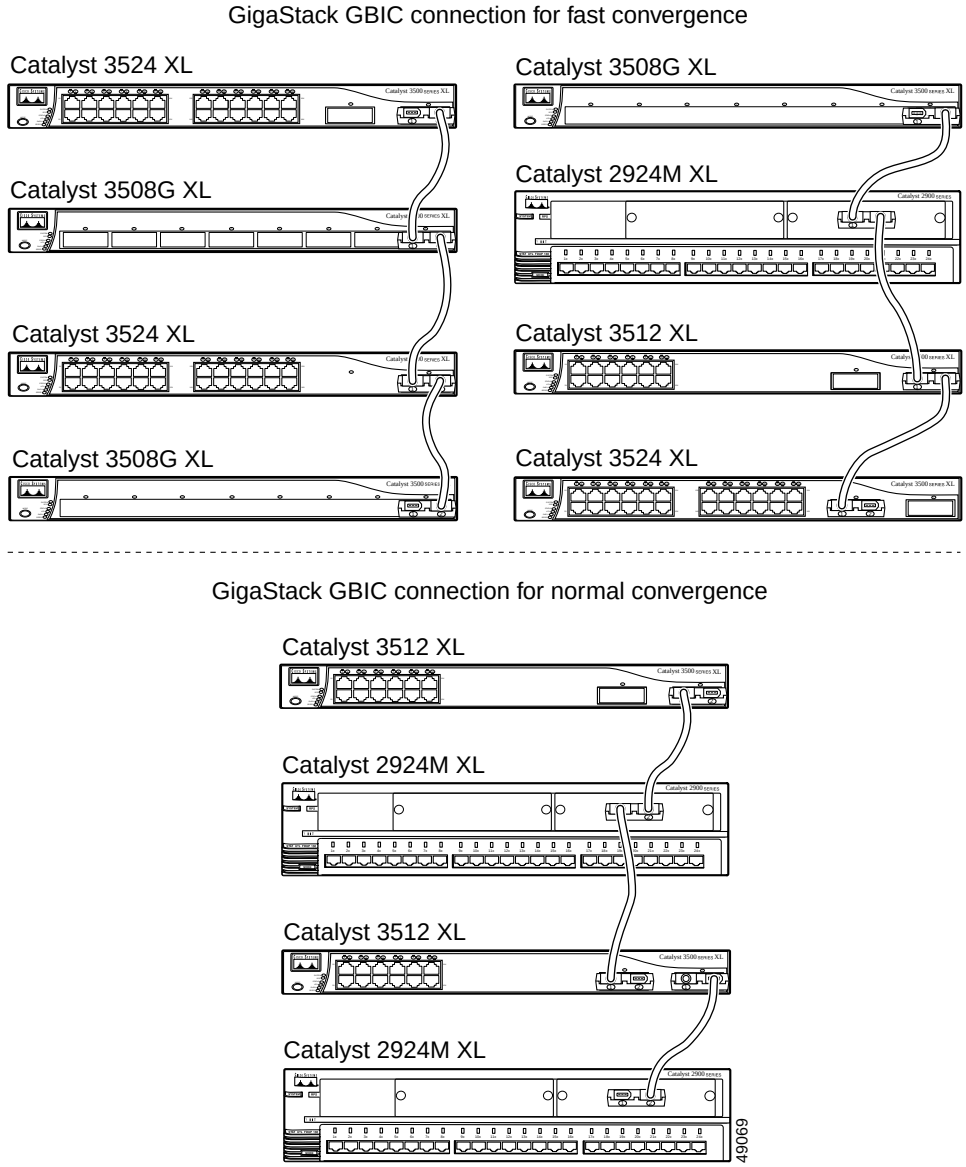
- CSUF runs on the Gigastack GBICs installed on Catalyst 3500 XL switches and installed in the 1000BaseX module on the modular Catalyst 2900 XL switches.
- Up to nine stack switches can be connected through their stack ports to the multidrop backbone. Only one stack port per switch is supported.
- Each stack switch can be connected to the STP backbone through one uplink.
- Up to 64 VLANs are supported.

Connecting the Stack Ports

A fast transition occurs across the stack of switches if the multidrop backbone connections are a continuous link from one GigaStack GBIC to another as shown in Figure 6-10. In addition, follow these guidelines:

- Do not connect alternate stack root ports to stack ports.
- Only one stack port is supported per switch.
- All stack ports on the stack of switches must be connected to the multidrop backbone.
- You can connect the open ports on the top and bottom GigaStack GBICs within the same stack to form a redundant link.

Figure 6-10 GigaStack GBIC Connections and STP Convergence



Configuring Cross-Stack UplinkFast

Before enabling CSUF, make sure your stack switches are properly connected. For more information, see the "Connecting the Stack Ports" section on page 6-40.

Beginning in privileged EXEC mode, follow these steps to enable CSUF:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**spanning-tree uplinkfast [max-update-rate** *pkts-per-second*]	Enable UplinkFast on the switch. (Optional) For **max-update-rate** *pkts-per-second, specify t*he number of packets per second at which update packets are sent. The range is 0 to 65535; the default is 150 packets per second.
Step 1	**interface** *interface-id*	Enter interface configuration mode, and specify the GBIC interface on which to enable CSUF.
Step 2	**spanning-tree stack-port**	Enable CSUF on only one stack-port GBIC interface. The stack port connects to GigaStack GBIC multidrop backbone. If you try to enable CSUF on a Fast Ethernet or a copper-based Gigabit Ethernet port, you receive an error message. If CSUF is already enabled on an interface and you try to enable it on another interface, you receive an error message. You must disable CSUF on the first interface before enabling it on a new interface. Use this command only on access switches.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show spanning-tree**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable CSUF on an interface, use the **no spanning-tree stack-port interface configuration** command. To disable UplinkFast on the switch, use the **no spanning-tree uplinkfast** global configuration command.

Changing the STP Parameters for a VLAN

The root switch for each VLAN is the switch with the highest priority and transmits topology frames to other switches in the spanning tree. You can change the root parameters for the VLANs on a selected switch. These options define how your switch responds when STP reconfigures itself.

Protocol	Implementation of STP to use: IBM or IEEE. The default is IEEE.
Priority	Value (0 to 65535) used to identify the root switch. The switch with the **lowest value** has the highest priority and is selected as the root.
Max age	Number of seconds (6 to 200) a switch waits without receiving STP configuration messages before attempting a reconfiguration. This parameter takes effect when a switch is operating as the root switch. Switches not acting as the root use the root-switch Max age parameter.
Hello Time	Number of seconds (1 to 10) between the transmission of hello messages, which mean that the switch is active. Switches not acting as a root switch use the root-switch Hello-time value.
Forward Delay	Number of seconds (4 to 200) a port waits before changing from its STP learning and listening states to the forwarding state. This wait is necessary so that other switches on the network ensure that no loop is formed before they allow the port to forward packets.

Changing the STP Implementation

Beginning in privileged EXEC mode, follow these steps to change the STP implementation. The *stp-list* is the list of VLANs to which the STP command applies.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**spanning-tree** [**vlan** *stp-list*] **protocol** {**ieee** | **ibm**}	Specify the STP implementation to be used for a spanning-tree instance.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show spanning-tree**	Verify your entry.

Changing the Switch Priority

Beginning in privileged EXEC mode, follow these steps to change the switch priority and affect which switch is the root switch. The *stp-list* is the list of VLANs to which the STP command applies.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**spanning-tree** [**vlan** *stp-list*] **priority** *bridge-priority*	Configure the switch priority for the specified spanning-tree instance. Enter a number from 0 to 65535; the lower the number, the more likely the switch will be chosen as the root switch.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show spanning-tree**	Verify your entry.

Changing the BPDU Message Interval

Beginning in privileged EXEC mode, follow these steps to change the BPDU message interval (max age time). The *stp-list* is the list of VLANs to which the STP command applies.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**spanning-tree** [**vlan** *stp-list*] **max-age** *seconds*	Specify the interval between messages the spanning tree receives from the root switch. The maximum age is the number of seconds a switch waits without receiving STP configuration messages before attempting a reconfiguration. Enter a number from 6 to 200.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show spanning-tree**	Verify your entry.

Changing the Hello BPDU Interval

Beginning in privileged EXEC mode, follow these steps to change the hello BPDU interval (hello time). The *stp-list* is the list of VLANs to which the STP command applies.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**spanning-tree** [**vlan** *stp-list*] **hello-time** *seconds*	Specify the interval between hello BPDUs. Hello messages show that the switch is active. Enter a number from 1 to 10.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show spanning-tree**	Verify your entry.

Changing the Forwarding Delay Time

Beginning in privileged EXEC mode, follow these steps to change the forwarding delay time. The *stp-list* is the list of VLANs to which the STP command applies.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**spanning-tree** [**vlan** *stp-list*] **forward-time** *seconds*	Specify the forwarding time for the specified spanning-tree instance. The forward delay is the number of seconds a port waits before changing from its STP learning and listening states to the forwarding state. Enter a number from 4 to 200. The default for IEEE is 15 seconds; the default for IBM is 4 seconds.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show spanning-tree**	Verify your entry.

STP Port States

When a port is not forwarding due to STP, it can be in one of these states:

- Blocking—Port is not participating in the frame-forwarding process and is not learning new addresses.
- Listening—Port is not participating in the frame-forwarding process, but is progressing towards a forwarding state. The port is not learning addresses.
- Learning—Port is not forwarding frames but is learning addresses.
- Forwarding—Port is forwarding frames and learning addresses.
- Disabled—Port has been removed from STP operation.
- Down—Port has no physical link.
- Broken—One end of the link is configured as an access port, and the other end is configured as an 802.1Q trunk port, or both ends of the link are configured as 802.1Q trunk ports but have different native VLAN IDs.

Enabling the Port Fast Feature

The Port Fast feature brings a port directly from a blocking state into a forwarding state. This feature is useful when a connected server or workstation times out because its port is going through the normal cycle of STP status changes. A port with Port Fast enabled only goes through the normal cycle of STP status changes when the switch is restarted.

Caution Enabling this feature on a port connected to a switch or hub could prevent STP from detecting and disabling loops in your network, and this could cause broadcast storms and address-learning problems.

You can modify these Port Fast parameters:

- Port Fast—Enable to bring the port more quickly to an STP forwarding state.
- Path Cost—A lower path cost represents higher-speed transmission. This can affect which port remains enabled in the event of a loop.

  Enter a number from 1 to 65535. The default is 100 for 10 Mbps, 19 for 100 Mbps, 14 for 155 Mbps (ATM), 4 for 1 Gbps, 2 for 10 Gbps, and 1 for interfaces with speeds greater than 10 Gbps.
- Priority—Number used to set the priority for a port. A higher number has higher priority. Enter a number from 0 to 65535.

Enabling this feature on a port connected to a switch or hub could prevent STP from detecting and disabling loops in your network.

Beginning in privileged EXEC mode, follow these steps to enable the Port Fast feature:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port to be configured.
Step 3	**spanning-tree portfast**	Enable the Port Fast feature for the port.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entry.

Changing the Path Cost

Beginning in privileged EXEC mode, follow these steps to change the path cost for STP calculations. The STP command applies to the *stp-list*.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port to be configured.
Step 3	**spanning-tree** [**vlan** *stp-list*] **cost** *cost*	Configure the path cost for the specified spanning-tree instance. Enter a number from 1 to 65535.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entry.

Changing the Port Priority

Beginning in privileged EXEC mode, follow these steps to change the port priority, which is used when two switches tie for position as the root switch. The *stp-list* is the list of VLANs to which the STP command applies.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port to be configured.
Step 3	**spanning-tree** [**vlan** *stp-list*] **port-priority** *port-priority*	Configure the port priority for a specified instance of STP. Enter a number from 0 to 255. The lower the number, the higher the priority.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entry.

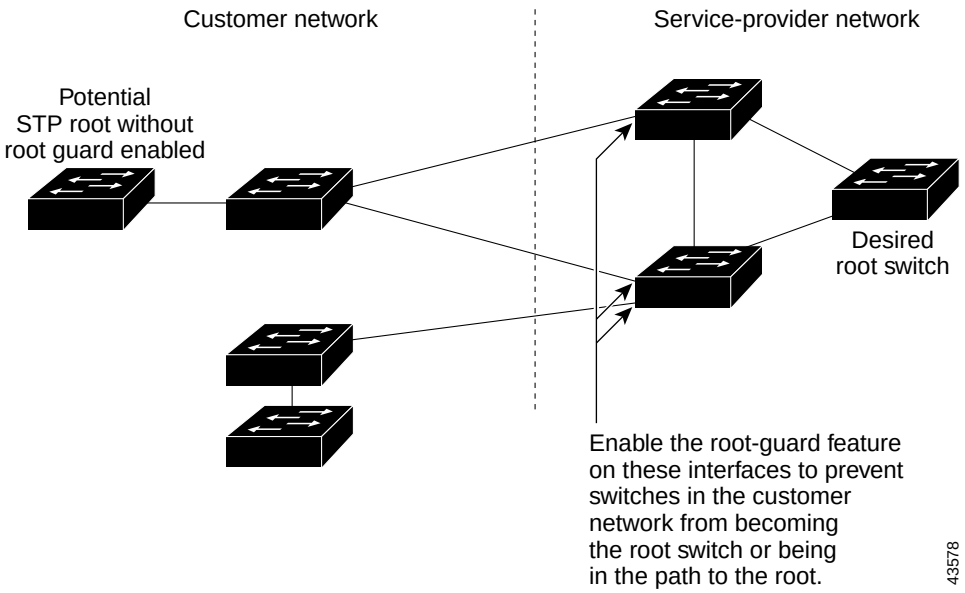
Configuring STP Root Guard

The Layer 2 network of a service provider (SP) can include many connections to switches that are not owned by the SP. In such a topology, STP can reconfigure itself and select a *customer switch* as the STP root switch, as shown in Figure 6-11. You can avoid this situation by configuring the root-guard feature on interfaces that connect to switches outside of your customer's network. If STP calculations cause an interface in the customer network to be selected as the root port, root guard then places the interface into the root-inconsistent (blocked) state to prevent the customer switch from becoming the root switch or being in the path to the root.

If a switch outside the network becomes the root switch, the interface is blocked (root-inconsistent state), and STP selects a new root switch. The customer switch does not become the root switch and is not in the path to the root.

Caution Misuse of this feature can cause a loss of connectivity.

Figure 6-11 STP in a Service Provider Network



Root guard enabled on a port applies to all the VLANs that the port belongs to. Each VLAN has its own instance of STP.

Beginning in privileged EXEC mode, follow these steps to set root guard on a port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port to be configured.
Step 3	**spanning-tree rootguard**	Enable root guard on the port.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify that the port is configured for root guard.

Use the **no** version of the **spanning-tree rootguard** command to disable the root guard feature.

Configuring SNMP

This software release supports these Simple Network Management Protocol (SNMP) versions:

- SNMPv1—The Simple Network Management Protocol, a Full Internet Standard, defined in RFC 1157.
- SNMPv2C, which has these features:
  - SNMPv2—Version 2 of the Simple Network Management Protocol, a Draft Internet Standard, defined in RFCs 1902 through 1907.
  - SNMPv2C—The Community-based Administrative Framework for SNMPv2, an Experimental Internet Protocol defined in RFC 1901.

You must configure the SNMP agent to use the version of SNMP supported by the management station. An agent can communicate with multiple managers; for this reason, you can configure the software to support communications with one management station using the SNMPv1 protocol and another using the SNMPv2 protocol.

Both SNMPv1 and SNMPv2C use a community-based form of security. The community of managers able to access the agent's MIB is defined by an IP address access control list and password.

SNMPv2C includes a bulk retrieval mechanism and more detailed error message reporting to management stations. The bulk retrieval mechanism retrieves tables and large quantities of information, minimizing the number of round-trips required. The SNMPv2C improved error-handling includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. Error return codes now report the error type.

SNMPv2C replaces the Party-based Administrative and Security Framework of SNMPv2Classic with the Community-based Administrative Framework of SNMPv2C while retaining the bulk retrieval and improved error handling of SNMPv2Classic.

Note If your switch is part of a cluster, the clustering software can change SNMP parameters (such as host names) when the cluster is created. If you are configuring a cluster for SNMP, see the "SNMP Community Strings" section on page 5-14.

Disabling and Enabling SNMP

SNMP is enabled by default and must be enabled for Cluster Management features to work properly.

SNMP is always enabled for Catalyst 1900 and Catalyst 2820 switches.

For CLI procedures, refer to the Cisco IOS Release 12.0 documentation on Cisco.com for additional information and CLI procedures.

Entering Community Strings

Community strings serve as passwords for SNMP messages, permitting access to the agent on the switch. If you are entering community strings for a cluster member, see the "SNMP Community Strings" section on page 5-14. You can enter community strings with these characteristics:

Read-only (RO)—Requests accompanied by the string can display MIB-object information.

Read-write (RW)—Requests accompanied by the string can display MIB-object information and set MIB objects.

For CLI procedures, refer to the Cisco IOS Release 12.0 documentation on Cisco.com for additional information and CLI procedures.

Adding Trap Managers

A trap manager is a management station that receives and processes traps. When you configure a trap manager, the community strings for each member switch must be unique. If a member switch has an assigned IP address, the management station accesses the switch by using that IP address.

By default, no trap manager is defined, and no traps are issued. Table 6-4 describes SNMP traps that you can configure on the the Catalyst 2900 XL and Catalyst 3500 XL. You can enable any or all of these traps and configure a trap manager on these switches to receive them.

Table 6-4 Catalyst 2900 XL and Catalyst 3500 XL SNMP Traps

c2900/C3500	Generate the switch-specific traps. These traps are in the private enterprise-specific Management Information Base (MIB).
c2900	Generate these traps: • Secure address violaton • Broadcast storm • RPS failed (power supply failure)
cluster	Generate cluster member status change traps.
config	Generate configuration management event traps and configuration copy traps.
hsrp	Generate Hot Standby Router Protocol (HSRP) state change traps.
mac-notification	Generate MAC notification event traps.
snmp	Generate coldstart, linkdown, linkup, and authentication failure traps.
tty	Generate management-console-CLI-session start traps.
vlan membership	Generate VLAN Membership Policy Server (VMPS) change traps.
vtp	Generate these VLAN Trunking Protocol (VTP) traps: • VTP configuration revision error • VTP configuration digest error • VTP server disabled error • VTP data too big error • vtpVlanRingNumberConfigConflict (for Token Ring only) • vtpVersionOneDeviceDetected • vlanTrunkPortDynamicStatusChange

Catalyst 1900 and Catalyst 2820 switches support up to four trap managers. When you configure community strings for these switches, limit the string length to 32 characters. When configuring traps on these switches, you cannot configure individual trap managers to receive specific traps.

Table 6-5 describes the Catalyst 1900 and Catalyst 2820 SNMP traps. You can enable any or all of these traps, but these traps are received by all configured trap managers.

Table 6-5 Catalyst 1900 and Catalyst 2820 SNMP Traps

Trap Type	Description
Address-violation	Generates a trap when the address violation threshold is exceeded.
Authentication	Generates a trap when an SNMP request is not accompanied by a valid community string.
BSC	Generates a trap when the broadcast threshold is exceeded.
Link-up-down	Generates a link-down trap when a port is suspended or disabled for any of these reasons: • Secure address violation (address mismatch or duplication) • Network connection error (loss of linkbeat or jabber error) • User disabling the port Generates a link-up trap when a port is enabled for any of these reasons: • Presence of linkbeat • Management intervention • Recovery from an address violation or any other error • STP action
VTP	Generates a trap when VTP changes occur.

Beginning in privileged EXEC mode, follow these steps to add a trap manager and a community string:

	Command	Purpose
Step 1	**config terminal**	Enter global configuration mode.
Step 2	**snmp-server host 172.2.128.263** *community-string* **snmp vlan-membership**	Enter the trap manager IP address, the community string, and the traps to generate.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify that the information was entered correctly by displaying the running configuration.

Configuring TACACS+

The Terminal Access Controller Access Control System Plus (TACACS+) provides the means to manage network security (authentication, authorization, and accounting [AAA]) from a server. This section describes how TACACS+ works and how you can configure it. For complete syntax and usage information for the commands described in this chapter, refer to the *Cisco IOS Release 12.0 Security Command Reference*.

You can only configure this feature by using the CLI; you cannot configure it through the Cluster Management Suite.

Note If TACACS+ is configured on the command switch, TACACS+ must also be configured on all member switches to access the switch cluster from CMS. For more information about switch clusters, see the Chapter 5, "Clustering Switches."

In large enterprise networks, the task of administering passwords on each device can be simplified by centralizing user authentication on a server. TACACS+ is an access-control protocol that allows a switch to authenticate all login attempts through a central server. The network administrator configures the switch with the address of the TACACS+ server, and the switch and the server exchange messages to authenticate each user before allowing access to the management console.

TACACS+ consists of three services: authentication, authorization, and accounting. Authentication determines who the user is and whether or not the user is allowed access to the switch. Authorization is the action of determining what the user is allowed to do on the system. Accounting is the action of collecting data related to resource usage.

The TACACS+ feature is disabled by default. However, you can enable and configure it by using the CLI. You can access the CLI through the console port or through Telnet. To prevent a lapse in security, you cannot configure TACACS+ through a network-management application. When enabled, TACACS+ can authenticate users accessing the switch through the CLI.

Note Although the TACACS+ configuration is performed through the CLI, the TACACS+ server authenticates HTTP connections that have been configured with a privilege level of 15.

Configuring the TACACS+ Server Host

Use the **tacacs-server host** command to specify the names of the IP host or hosts maintaining an AAA/TACACS+ server. On TACACS+ servers, you can configure these additional options:

- Number of seconds that the switch waits while trying to contact the server before timing out.
- Encryption key to encrypt and decrypt all traffic between the router and the daemon.
- Number of attempts that a user can make when entering a command that is being authenticated by TACACS+.

Beginning in privileged EXEC mode, follow these steps to configure the TACACS+ server:

	Command	Purpose
Step 1	**tacacs-server host** *name* [**timeout** *integer*] [**key** *string*]	Define a TACACS+ host. Entering the **timeout** and **key** parameters with this command overrides the global values that you can enter with the **tacacs-server timeout** (Step 3) and the **tacacs-server key** commands (Step 5).
Step 2	**tacacs-server retransmit** *retries*	Enter the number of times the server searches the list of TACACS+ servers before stopping. The default is two.
Step 3	**tacacs-server timeout** *seconds*	Set the interval that the server waits for a TACACS+ server host to reply. The default is 5 seconds.
Step 4	**tacacs-server attempts** *count*	Set the number of login attempts that can be made on the line.
Step 5	**tacacs-server key** *key*	Define a set of encryption keys for all of TACACS+ and communication between the access server and the TACACS daemon. Repeat the command for each encryption key.
Step 6	**exit**	Return to privileged EXEC mode.
Step 7	**show tacacs**	Verify your entries.

Configuring Login Authentication

Beginning in privileged EXEC mode, follow these steps to configure login authentication by using AAA/TACACS+:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa new-model**	Enable AAA/TACACS+.
Step 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	Enable authentication at login, and create one or more lists of authentication methods.
Step 4	**line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]	Enter line configuration mode, and configure the lines to which you want to apply the authentication list.
Step 5	**login authentication** {**default** | *list-name*}	Apply the authentication list to a line or set of lines.
Step 6	**exit**	Return to privileged EXEC mode.
Step 7	**show running-config**	Verify your entries.

The variable *list-name* is any character string used to name the list you are creating. The *method* variable refers to the actual methods the authentication algorithm tries, in the sequence entered. You can choose one of these methods:

- **line**—Uses the line password for authentication. You must define a line password before you can use this authentication method. Use the **password** *password* line configuration command.
- **local**—Uses the local username database for authentication. You must enter username information into the database. Use the **username** *password* global configuration command.
- **tacacs+—**Uses TACACS+ authentication. You must configure the TACACS+ server before you can use this authentication method. For more information, see the "Configuring the TACACS+ Server Host" section on page 6-51.

To create a default list that is used if **no list** is specified in the **login authentication** line configuration command, use the **default** keyword followed by the methods you want used in default situations.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication succeed even if all methods return an error, specify **none** as the final method in the command line.

Specifying TACACS+ Authorization for EXEC Access and Network Services

You can use the **aaa authorization** global configuration command with the **tacacs+** keyword to set parameters that restrict a user's network access to Cisco IOS privilege mode (EXEC access) and to network services such as Serial Line Internet Protocol (SLIP), Point-to-Point Protocol (PPP) with Network Control Protocols (NCPs), and AppleTalk Remote Access (ARA).

The **aaa authorization exec tacacs+ local** command sets these authorization parameters:

- Uses TACACS+ for EXEC access authorization if authentication was done using TACACS+.
- Uses the local database if authentication was not done using TACACS+.

Note Authorization is bypassed for authenticated users who login through the CLI even if authorization has been configured.

Beginning in privileged EXEC mode, follow these steps to specify TACACS+ authorization for EXEC access and network services:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa authorization network tacacs+**	Configure the switch for user TACACS+ authorization for all network-related service requests.
Step 3	**aaa authorization exec tacacs+**	Configure the switch for user TACACS+ authorization to determine if the user is allowed EXEC access. The **exec** keyword might return user profile information (such as **autocommand** information).
Step 4	**exit**	Return to privileged EXEC mode.

Starting TACACS+ Accounting

You use the **aaa accounting** command with the **tacacs+** keyword to turn on TACACS+ accounting for each Cisco IOS privilege level and for network services.

Beginning in privileged EXEC mode, follow these steps to enable TACACS+ accounting:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa accounting exec start-stop tacacs+**	Enable TACACS+ accounting to send a start-record accounting notice at the beginning of an EXEC process and a stop-record at the end.
Step 3	**aaa accounting network start-stop tacacs+**	Enable TACACS+ accounting for all network-related service requests, including SLIP, PPP, and PPP NCPs.
Step 4	**exit**	Return to privileged EXEC mode.

Note These commands are documented in the "Accounting and Billing Commands" chapter of the *Cisco IOS Release 12.0 Security Command Reference*.

Configuring a Switch for Local AAA

You can configure AAA to operate without a server by setting the switch to implement AAA in local mode. The switch then verifies authentication and authorization. No accounting is available in this configuration.

Beginning in privileged EXEC mode, follow these steps to configure the switch for local AAA:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa new-model**	Enable AAA.
Step 3	**aaa authentication login default local**	Set the login authorization to default to local.
Step 4	**aaa authorization exec local**	Configure user AAA authorization for all network-related service requests.
Step 5	**aaa authorization network local**	Configure user AAA authorization to determine if the user is allowed to run an EXEC shell.
Step 6	**username** *name* **privilege** *level* **password** *password*	Enter the local database. Repeat this command for each user.

Configuring the Switch Ports

This chapter provides these topics about changing the switch port settings:

- Changing the Port Speed and Duplex Mode, page 7-2
- Configuring Flooding Controls, page 7-4
- Configuring UniDirectional Link Detection, page 7-7
- Creating EtherChannel Port Groups, page 7-8
- Configuring Protected Ports, page 7-10
- Enabling Port Security, page 7-11
- Configuring SPAN, page 7-13
- Configuring Voice Ports, page 7-14
- Configuring Inline Power on the Catalyst 3524-PWR Ports, page 7-17

Note Certain port features can conflict with one another. Review the "Avoiding Configuration Conflicts" section on page 9-2 before you change the port settings.

For information about configuring these settings from Cluster Management Suite (CMS), refer to the online help.

This switch software release is based on Cisco IOS Release 12.0. It has been enhanced to support a set of features for the Catalyst 2900 XL and Catalyst 3500 XL switches. This chapter provides procedures for using only the commands that have been created or changed for these switches. The *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference* provides complete descriptions of these commands. This guide does not provide Cisco IOS Release 12.0 commands and information already documented in the Cisco IOS Release 12.0 documentation on Cisco.com.

For information about configuring these settings from Cluster Management Suite (CMS), refer to the online help.

Changing the Port Speed and Duplex Mode

Caution If you reconfigure the port through which you are managing the switch, a Spanning Tree Protocol (STP) reconfiguration could cause a temporary loss of connectivity.

Follow these guidelines when configuring the duplex and speed settings:

- Gigabit Ethernet ports are always set to 1000 Mbps but can negotiate full or half duplex with the attached device.
- Gigabit Ethernet ports that do not match the settings of an attached device lose connectivity and do not generate statistics.
- Asynchronous Transfer Mode (ATM) ports are always set to full duplex and do not autonegotiate duplex or speed settings.
- GigaStack-to-GigaStack stack connections operate in half-duplex mode, and GigaStack-to-GigaStack point-to-point connections operate in full-duplex mode.
- If STP is enabled, the switch can take up to 30 seconds to check for loops when a port is reconfigured. The port LED is amber while STP reconfigures.

Connecting to Devices That Do Not Autonegotiate

To connect to a remote 100BASE-T device that does not autonegotiate, set the duplex setting to **Full** or **Half**, and set the speed setting to **Auto**. Autonegotiation for the speed setting selects the correct speed even if the attached device does not autonegotiate, but the duplex setting must be explicitly set.

To connect to a remote Gigabit Ethernet device that does not autonegotiate, disable autonegotiation on the local device, and set the duplex and flow control parameters to be compatible with the other device.

Setting Speed and Duplex Parameters

Beginning in privileged EXEC mode, follow these steps to set the speed and duplex parameters on a 10/100 port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port to be configured.
Step 3	**speed** {**10** | **100** | **auto**}	Enter the speed parameter for the port. You cannot enter the speed on Gigabit Ethernet or ATM ports.
Step 4	**duplex** {**full** | **half** | **auto**}	Enter the duplex parameter for the port.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show running-config**	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entry in the configuration file. This retains the configuration when the switch restarts.

Configuring Flow Control on Gigabit Ethernet Ports

Beginning in privileged EXEC mode, follow these steps to configure flow control on a Gigabit Ethernet port.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port to be configured.
Step 3	**flowcontrol** [**asymmetric** | **symmetric**]	Configure flow control for the port.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entry in the configuration file. This retains the configuration when the switch restarts.

Configuring Flooding Controls

You can use these flooding techniques to block the forwarding of unnecessary flooded traffic:

- Enable storm control for unicast, multicast, or broadcast packets
- Block the forwarding of unicast and broadcast packets on a per-port basis
- Flood all unknown packets to a network port (configured only by using CLI)

Enabling Storm Control

A packet storm occurs when a large number of broadcast, unicast, or multicast packets are received on a port. Forwarding these packets can cause the network to slow down or to time out. Storm control is configured for the switch as a whole but operates on a per-port basis. By default, storm control is disabled.

Storm control uses high and low thresholds to block and then restore the forwarding of broadcast, unicast, or multicast packets. You can also set the switch to shut down the port when the rising threshold is reached.

The rising threshold is the number of packets that a switch port can receive before forwarding is blocked. The falling threshold is the number of packets below which the switch resumes normal forwarding. In general, the higher the threshold, the less effective the protection against broadcast storms. The maximum half-duplex transmission on a 100BASE-T link is 148,000 packets per second, but you can enter a threshold of up to 4294967295 broadcast packets per second.

Beginning in privileged EXEC mode, follow these steps to enable broadcast-storm control. (To enable storm control on multicast packets, use the **port storm-control multicast** command. To enable storm control on unicast packets, use the **port storm-control unicast** command.)

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port to configure.
Step 3	**port storm-control broadcast** [**threshold** {**rising** *rising-number* **falling** *falling-number*}]	Enter the rising and falling thresholds for broadcast packets. Make sure the rising threshold is greater than the falling threshold.
Step 4	**port storm-control trap**	Generate an SNMP trap when the traffic on the port crosses the rising or falling threshold.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show port storm-control** [*interface*]	Verify your entries.

Disabling Storm Control

Beginning in privileged EXEC mode, follow these steps to disable broadcast-storm control.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port to configure.
Step 3	**no port storm-control broadcast**	Disable port storm control.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show port storm-control** [*interface*]	Verify your entries.

Blocking Flooded Traffic on a Port

By default, the switch floods packets with unknown destination MAC addresses to all ports. Some configurations do not require flooding. For example, a port that has only manually assigned addresses has no unknown destinations, and flooding serves no purpose. Therefore, you can disable the flooding of unicast and multicast packets on a per-port basis. Ordinarily, flooded traffic does not cross VLAN boundaries, but multi-VLAN ports flood traffic to all VLANs they belong to.

Beginning in privileged EXEC mode, follow these steps to disable the flooding of multicast and unicast packets to a port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port to configure.
Step 3	**port block multicast**	Block unknown multicast forwarding to the port.
Step 4	**port block unicast**	Block unknown unicast flooding to the port.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show port block** {**multicast** | **unicast**} *interface*	Verify your entries, entering the appropriate command once for the **multicast** option and once for the **unicast** option.

Resuming Normal Forwarding on a Port

Beginning in privileged EXEC mode, follow these steps to resume normal forwarding on a port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port to configure.
Step 3	**no port block multicast**	Enable unknown multicast forwarding to the port.
Step 4	**no port block unicast**	Enable unknown unicast flooding to the port.
Step 5	**end**	Return to privileged EXEC mode
Step 6	**show port block** {**multicast** | **unicast**} *interface*	Verify your entries, entering the appropriate command once for the **multicast** option and once for the **unicast** option.

Enabling a Network Port

Network ports are assigned per VLAN and can reduce flooded traffic on your network. The switch forwards all traffic with unknown destination addresses to the network port instead of flooding the traffic to all ports in the VLAN.

When you configure a port as the network port, the switch deletes all associated addresses from the address table and disables learning on the port. If you configure other ports in the VLAN as secure ports, the addresses on those ports are not aged. If you move a network port to a VLAN without a network port, it becomes the network port for the new VLAN.

You cannot change the settings for unicast and multicast flooding on a network port. You can assign only one network port per VLAN. For the restrictions that apply to a network port, see the "Assigning Passwords and Privilege Levels" section on page 6-11.

Caution A network port cannot link cluster members.

Beginning in privileged EXEC mode, follow these steps to define a network port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port to be configured.
Step 3	**port network**	Define the port as the network port.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entry.

Disabling a Network Port

Beginning in privileged EXEC mode, follow these steps to disable a network port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port to be configured.
Step 3	**no port network**	Disable the port as the network port.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entry.

Configuring UniDirectional Link Detection

UniDirectional Link Detection (UDLD) is a Layer 2 protocol that detects and shuts down unidirectional links. You can configure UDLD on the entire switch or on an individual port. Use the **udld reset** command to reset all ports that have been shut down by UDLD.

Beginning in privileged EXEC mode, follow these steps to configure UDLD on a switch:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**udld enable**	Enable UDLD on all switch ports. Use the **udld** interface configuration command to enable UDLD on a specific port.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify the entry by displaying the running configuration.

Creating EtherChannel Port Groups

Fast EtherChannel (FEC) and Gigabit EtherChannel port groups act as single, logical ports for high-bandwidth connections between switches or between switches and servers.

Note You can create port groups of either Gigabit Ethernet ports or 100BASE-TX ports, but you cannot create a port group that has both port speeds.

For the restrictions that apply to port groups, see the "Avoiding Configuration Conflicts" section on page 9-2.

Understanding EtherChannel Port Grouping

This software release supports two different types of port groups: source-based forwarding port groups and destination-based forwarding port groups.

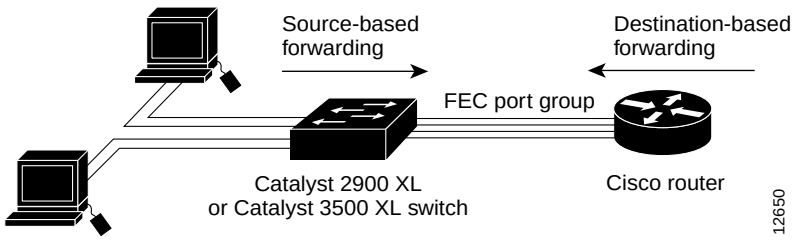
Source-based forwarding port groups distribute packets forwarded to the group based on the source address of incoming packets. You can configure up to eight ports in a source-based forwarding port group. Source-based forwarding is enabled by default.

Destination-based port groups distribute packets forwarded to the group based on the destination address of incoming packets. You can configure an unlimited number of ports in a destination-based port group.

You can create up to 12 port groups. All ports in each group must be of the same type; for example, they must be all source-based or all destination-based. You can have source-based port groups and destination-based source groups. You can independently configure port groups that link switches, but you must consistently configure both ends of a port group.

In Figure 7-1, a port group of two workstations communicates with a router. Because the router is a single-MAC-address device, source-based forwarding ensures that the switch uses all available bandwidth to the router. The router is configured for destination-based forwarding because the large number of stations ensures that the traffic is evenly distributed through the port-group ports on the router.

Figure 7-1 Source-Based Forwarding



The switch treats the port group as a single logical port; therefore, when you create a port group, the switch uses the configuration of the first port for all ports added to the group. If you add a port and change the forwarding method, it changes the forwarding for all ports in the group. After the group is created, changing STP or VLAN membership parameters for one port in the group automatically changes the parameters for all ports. Each port group has one port that carries all unknown multicast, broadcast, and STP packets.

Port Group Restrictions on Static-Address Forwarding

These restrictions apply to entering static addresses that are forwarded to port groups:

- If the port group forwards based on the source MAC address (the default), configure the static address to forward to all ports in the group. This method eliminates the chance of lost packets.
- If the port group forwards based on the destination address, configure the static address to forward to only one port in the port group. This method avoids the possible transmission of duplicate packets. For more information, see the "Adding Static Addresses" section on page 6-19.

Creating EtherChannel Port Groups

Beginning in privileged EXEC mode, follow these steps to create a two-port group:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port of the first port to be added to the group.
Step 3	**port group 1 distribution destination**	Assign the port to group 1 with destination-based forwarding.
Step 4	**interface** *interface*	Enter the second port to be added to the group.
Step 5	**port group 1 distribution destination**	Assign the port to group 1 with destination-based forwarding.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show running-config**	Verify your entries.

Configuring Protected Ports

Some applications require that no traffic be forwarded by the Layer 2 protocol between ports on the same switch. In such an environment, there is no exchange of unicast, broadcast, or multicast traffic between ports on the switch, and traffic between ports on the same switch is forwarded through a Layer 3 device such as a router.

To meet this requirement, you can configure Catalyst 2900 XL and Catalyst 3500 XL ports as protected ports (also referred to as private VLAN edge ports). Protected ports do not forward any traffic to protected ports on the same switch. This means that all traffic passing between protected ports—unicast, broadcast, and multicast—must be forwarded through a Layer 3 device. Protected ports can forward any type of traffic to unprotected ports, and they forward as usual to all ports on other switches.

Note Sometimes unknown unicast traffic from an unprotected port is flooded to a protected port because a MAC address has timed out or has not been learned by the switch. Use the **port block** command to guarantee that in such a case no unicast and multicast traffic is flooded to the port. See the "Configuring Flooding Controls" section on page 7-4 for more information.

Beginning in privileged EXEC mode, follow these steps to define a port as a protected port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port to be configured.
Step 3	**port protected**	Enable protected port on the port.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show port protected**	Verify that the protected port option is enabled.

Use the **no** version of the **port protected** interface configuration command to disable the protected port option.

Enabling Port Security

Secured ports restrict a port to a user-defined group of stations. When you assign secure addresses to a secure port, the switch does not forward any packets with source addresses outside the group of addresses you have defined. If you define the address table of a secure port to contain only one address, the workstation or server attached to that port is guaranteed the full bandwidth of the port. As part of securing the port, you can also define the size of the address table for the port.

Secured ports generate address-security violations under these conditions:

- The address table of a secured port is full and the address of an incoming packet is not found in the table.
- An incoming packet has a source address assigned as a secure address on another port.

Limiting the number of devices that can connect to a secure port has these advantages:

- Dedicated bandwidth—If the size of the address table is set to 1, the attached device is guaranteed the full bandwidth of the port.
- Added security—Unknown devices cannot connect to the port.

These options validate port security or indicate security violations:

Interface	Port to secure.
Security	Enable port security on the port.
Trap	Issue a trap when an address-security violation occurs.
Shutdown Port	Disable the port when an address-security violation occurs.
Secure Addresses	Number of addresses in the address table for this port. Secure ports have at least one address.
Max Addresses	Number of addresses that the address table for the port can contain.
Security Rejects	The number of unauthorized addresses seen on the port.

For the restrictions that apply to secure ports, see the "Avoiding Configuration Conflicts" section on page 9-2.

Defining the Maximum Secure Address Count

A secure port can have from 1 to 132 associated secure addresses. Setting one address in the MAC address table for the port ensures that the attached device has the full bandwidth of the port.

Enabling Port Security

Beginning in privileged EXEC mode, follow these steps to enable port security.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode for the port you want to secure.
Step 3	**port security max-mac-count 1**	Secure the port and set the address table to one address.
Step 4	**port security action shutdown**	Set the port to shutdown when a security violation occurs.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show port security**	Verify the entry.

Disabling Port Security

Beginning in privileged EXEC mode, follow these steps to disable port security.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode for the port you want to disable port security.
Step 3	**no port security**	Disable port security.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show port security**	Verify the entry.

Configuring SPAN

You can use Switch Port Analyzer (SPAN) to monitor traffic on a given port by forwarding incoming and outgoing traffic on the port to another port in the same VLAN. A SPAN port cannot monitor ports in a different VLAN, and a SPAN port must be a static-access port. You can define any number of ports as SPAN ports, and any combination of ports can be monitored.

For the restrictions that apply to SPAN ports, see the "Avoiding Configuration Conflicts" section on page 9-2.

Enabling SPAN

Beginning in privileged EXEC mode, follow these steps to enable SPAN:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port that acts as the monitor port.
Step 3	**port monitor** *interface*	Enable port monitoring on the port.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.

Disabling SPAN

Beginning in privileged EXEC mode, follow these steps to disable SPAN:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port number of the monitor port.
Step 3	**no port monitor** *interface*	Disable port monitoring on the port.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.

Configuring Voice Ports

The Catalyst 2900 XL and Catalyst 3500 XL switches can connect to a Cisco 7960 IP Phone and carry IP voice traffic. If necessary, the Catalyst 3524-PWR XL can supply electrical power to the circuit connecting it to the Cisco 7960 IP Phone.

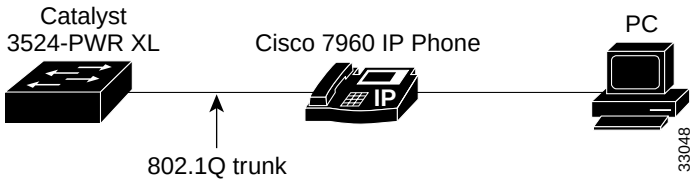
Because the sound quality of an IP telephone call can deteriorate if the data is unevenly transmitted, this release of IOS supports quality of service (QoS) based on IEEE 802.1p class of service (CoS). QoS uses classification and scheduling to transmit network traffic from the switch in a predictable manner. The Cisco 7960 IP Phone itself is also a configurable device, and you can configure it to forward traffic with an 802.1p priority. You can use the CLI to configure the Catalyst 3524-PWR XL to honor or ignore a traffic priority assigned by a Cisco 7960 IP Phone.

The Cisco 7960 IP Phone contains an integrated three-port 10/100 switch. The ports are dedicated connections to these devices:

- Port 1 connects to the Catalyst 3524-PWR XL switch or other voice-over-IP device.
- Port 2 is an internal 10/100 interface that carries the phone traffic.
- Port 3 connects to a PC or other device.

Figure 7-2 shows one way to configure a Cisco 7960 IP Phone.

Figure 7-2 Cisco 7960 IP Phone Connected to a Catalyst 3524-PWR XL Switch



Preparing a Port for a Cisco 7960 IP Phone Connection

Before you configure a Catalyst 3524-PWR XL port to carry IP voice traffic, configure the port as an 802.1Q trunk and as a member of the voice VLAN (VVID). See the "Configuring a Trunk Port" section on page 8-27 for instructions.

Configuring a Port to Connect to a Cisco 7960 IP Phone

Because a Cisco 7960 IP Phone also supports connection to a PC or other device, a port connecting a Catalyst 3524-PWR XL switch to a Cisco 7960 IP Phone can carry mixed traffic. There are three configurations for a port connected to a Cisco 7960 IP Phone:

- All traffic is transmitted according to the default COS priority of the port. This is the default.
- Voice traffic is given a higher priority by the phone, and all traffic is in the same VLAN.
- Voice and data traffic are carried on separate VLANs, and voice traffic always has a CoS priority of 5.

Beginning in privileged EXEC mode, follow these steps to configure a port to instruct the phone to give voice traffic a higher priority and to forward all traffic through the 802.1Q native VLAN.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port to be configured.
Step 3	**switchport voice vlan dot1p**	Instruct the switch port to use 802.1p priority tagging for voice traffic and to use VLAN 0 (default native VLAN) to carry all traffic.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show interface** *interface* **switchport**	Verify the port configuration.

Overriding the CoS Priority of Incoming Frames

A PC or other data device can connect to a Cisco 7960 IP Phone port. The PC can generate packets with an assigned CoS value. If you want, you can use the Catalyst 3524-PWR XL CLI to override the priority of frames arriving on the phone port from connected devices. You can also set the phone port to accept (trust) the priority of frames arriving on the port.

Beginning in privileged EXEC mode, follow these steps to override the CoS priority setting received from the non-voice port on the Cisco 7960 IP Phone:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the switch port to be configured.
Step 3	**switchport priority extend cos 3**	Set the phone port to override the priority received from the PC or the attached device and forward the received data with a priority of 3.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show interface** *interface* **switchport**	Verify the change.

Use the **no switchport priority extend** command to return the port to its default setting.

Configuring Voice Ports to Carry Voice and Data Traffic on Different VLANs

The Cisco 7960 IP Phone has an integrated three-port 10/100 switch that can connect to a PC or other device. You can configure a switch port to instruct the phone to forward voice and data traffic on different virtual LANs (VLANs).

In this configuration, VLAN 1 carries data traffic, and VLAN 2 carries voice traffic. In this configuration, you must connect all Cisco IP Phones and other voice-related devices to switch ports that belong to VLAN 2.

Beginning in privileged EXEC mode, follow these steps to configure a port to receive voice and data from a Cisco IP Phone in different VLANs:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port to be configured.
Step 3	**switchport priority default (0)**	Assign an IEEE 802.1p priority to untagged traffic that is received on the switch port. The Cisco IP Phone forwards this traffic through the native VLAN, VLAN 1.
Step 4	**switchport voice vlan (2)**	Instruct the Cisco IP Phone to forward all voice traffic through VLAN 2. The Cisco IP Phone forwards the traffic with an 802.1p priority of 5.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show interface** *interface* **switchport**	Verify the configuration.

Configuring Inline Power on the Catalyst 3524-PWR Ports

The Catalyst 3524-PWR XL can supply inline power to the Cisco 7960 IP Phone, if necessary. The Cisco 7960 IP Phone can also be connected to an AC power source and supply its own power to the voice circuit. When the Cisco 7960 IP Phone supplies its own power, any Catalyst 2900 XL or Catalyst 3500 XL can forward IP voice traffic to and from the phone.

The Catalyst 3524-PWR XL senses if it is connected to a Cisco 7960 IP Phone. If there is *no* power on the circuit, the switch supplies the power. If there is power on the circuit, the switch does not supply it.

You can configure the switch to never supply power to the Cisco 7960 IP Phone and to disable the detection mechanism. See the "Configuring Voice Ports" section on page 7-14 for the CLI commands that you use to supply inline power to a Cisco 7960 IP Phone.

Beginning in privileged EXEC mode, follow these steps to configure a port to never supply power to Cisco 7960 IP Phones.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port to be configured.
Step 3	**power inline never**	Permanently disable inline power on the port. To enable inline power when a Cisco 7960 IP Phone is detected, use the **power inline auto** command.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show power inline** *interface* **configured**	Verify the change.

Configuring VLANs

This chapter provides these topics about configuring virtual LANs (VLANs):

- Overview, page 8-2
- Management VLANs, page 8-3
- Assigning VLAN Port Membership Modes, page 8-5
- Assigning Static-Access Ports to a VLAN, page 8-7
- Overlapping VLANs and Multi-VLAN Ports, page 8-7
- Using VTP, page 8-9
- VLANs in the VTP Database, page 8-19
- How VLAN Trunks Work, page 8-25
- Configuring 802.1p Class of Service, page 8-30
- Load Sharing Using STP, page 8-31
- How the VMPS Works, page 8-35

Note Certain port features can conflict with one another. Review the "Avoiding Configuration Conflicts" section on page 9-2 before you change the port settings.

For information about configuring these settings from Cluster Management Suite (CMS), refer to the online help.

This switch software release is based on Cisco IOS Release 12.0. It has been enhanced to support a set of features for the Catalyst 2900 XL and Catalyst 3500 XL switches. This chapter provides procedures for using only the commands that have been created or changed for these switches. The *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference* provides complete descriptions of these commands. This guide does not provide Cisco IOS Release 12.0 commands and information already documented in the Cisco IOS Release 12.0 documentation on Cisco.com.

For information about configuring these settings from Cluster Management Suite (CMS), refer to the online help.

Overview

A virtual LAN (VLAN) is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to stations in the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router or bridge as shown in Figure 8-1. VLANs are identified with a number of 1 to 1001.

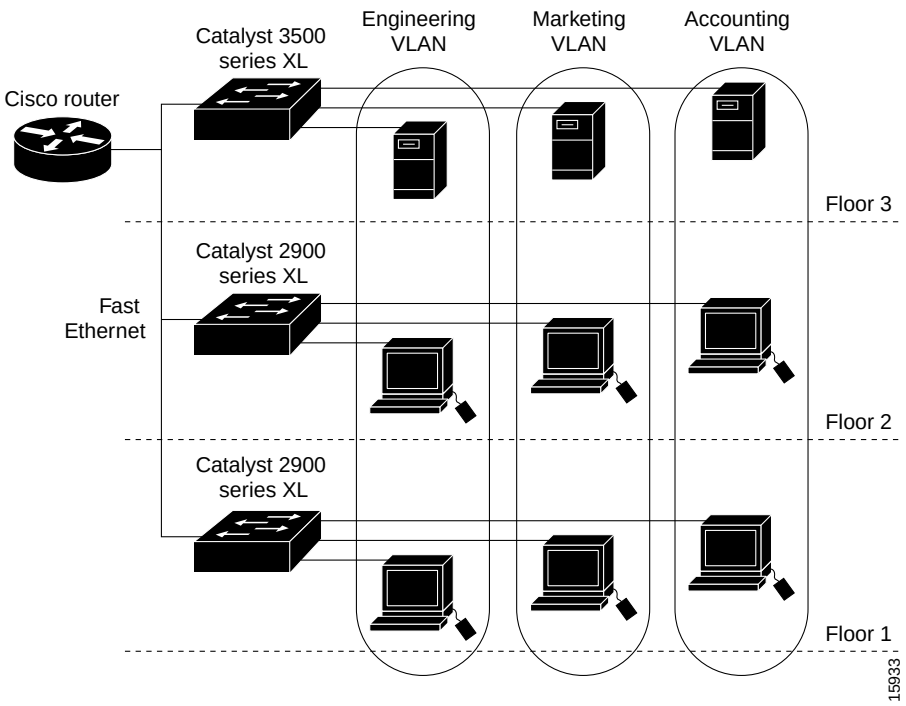
Because a VLAN is considered a separate logical network, it contains its own bridge Management Information Base (MIB) information and can support its own implementation of the Spanning Tree Protocol (STP). For information about managing VLAN STP instances, see the "Supported STP Instances" section on page 6-33.

Table 8-1 lists the number of supported VLANs and STP instances on the switches.

Table 8-1 Maximum Number of Supported VLANs

Switch	Maximum Number of VLANs	Maximum Number of STP Instances	Trunking Supported?
Catalyst 2912 XL, Catalyst 2924 XL, and Catalyst 2924C XL switches	64	64	Yes
Catalyst 2900 LRE XL switches	250	64	Yes
Catalyst 2912M and Catalyst 2924M modular switches	250	64	Yes
Catalyst 3500 XL switches	250	64	Yes

Figure 8-1 VLANs as Logically Defined Networks



The switches in Table 8-1 support both Inter-Switch Link (ISL) and IEEE 802.1Q trunking methods for transmitting VLAN traffic over 100BASE-T and Gigabit Ethernet ports.

The GigaStack GBIC also supports both trunking methods. When you are configuring a cascaded stack of Catalyst 3500 XL switches using the GigaStack GBIC and want to include more than one VLAN in the stack, be sure to configure all of the GigaStack GBIC interfaces as trunk ports by using the **switchport mode trunk** interface configuration command and to use the same encapsulation method by using the **switchport encapsulation** {**isl** | **dot1q**} interface configuration command. For more information on these commands, refer to the *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference*.

Trunking is supported on all 8-MB switches running Cisco IOS 12.0(5)XP and later. Trunking is not supported on some older software releases and on some older Catalyst 2900 XL switches and modules. For information about which older devices and software releases support trunking, refer to the release notes for Release 11.2(8)SA6 or earlier (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm).

Management VLANs

Communication with the switch management interfaces is through the switch IP address. The IP address is associated with the management VLAN, which by default is VLAN 1.

The management VLAN has these characteristics:

- It is created from CMS or through the CLI on static-access, multi-VLAN, and dynamic-access and trunk ports. You cannot create or remove the management VLAN through Simple Network Management Protocol (SNMP).
- Only one management VLAN can be administratively active at a time.
- With the exception of VLAN 1, the management VLAN can be deleted.
- When created, the management VLAN is administratively down.

Before changing the management VLAN on your switch network, make sure you follow these guidelines:

- The new management VLAN should not have an Hot Standby Router Protocol (HSRP) standby group configured on it.
- You must be able to move your network management station to a switch port assigned to the same VLAN as the new management VLAN.
- Connectivity through the network must exist from the network management station to all switches involved in the management VLAN change.
- Switches running a version of IOS software that is earlier than Cisco IOS 12.0(5)XP cannot change the management VLAN.
- Switches running Cisco IOS 12.0(5)XP should be upgraded to the current software release as described in the release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm).

If you are using SNMP or CMS to manage the switch, ensure that the port through which you are connected to a switch is in the management VLAN.

For information about the role management VLANs play in switch clusters, see the "Management VLAN" section on page 5-16.

Changing the Management VLAN for a New Switch

If you add a new switch to an existing cluster and the cluster is using a management VLAN other than the default VLAN 1, the command switch automatically senses that the new switch has a different management VLAN and has not been configured. The command switch issues commands to change the management VLAN on the new switch to match the one in use by the cluster. This automatic change of the VLAN only occurs for new, out-of-box switches that do not have a config.text file and for which there have been no changes to the running configuration.

Before a new switch can be added to a cluster, it must be connected to a port that belongs to the cluster management VLAN. If the cluster is configured with a management VLAN other than the default, the command switch changes the management VLAN for new switches when they are connected to the cluster. In this way, the new switch can exchange CDP messages with the command switch and be proposed as a cluster candidate.

Note For the command switch to change the management VLAN on a new switch, there must have been no changes to the new switch configuration, and there must be no config.text file.

Because the switch is new and unconfigured, its management VLAN is changed to the cluster management VLAN when it is first added to the cluster. All ports that have an active link at the time of this change become members of the new management VLAN.

For information about the role management VLANs play in switch clusters, see the "Management VLAN" section on page 5-16.

Changing the Management VLAN Through a Telnet Connection

Before you start, review the "Management VLANs" section on page 8-3. Beginning in privileged EXEC mode on the command switch, follow these steps to configure the management VLAN interface through a Telnet connection:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**cluster management-vlan** *vlanid*	Change the management VLAN for the cluster. This ends your Telnet session. Move the port through which you are connected to the switch to a port in the new management VLAN.
Step 3	**show running-config**	Verify the change.

Assigning VLAN Port Membership Modes

You configure a port to belong to a VLAN by assigning a membership mode that determines the kind of traffic the port carries and the number of VLANs it can belong to. Table 8-2 lists the membership modes and characteristics.

Table 8-2 Port Membership Modes

Membership Mode	VLAN Membership Characteristics
Static-access	A static-access port can belong to one VLAN and is manually assigned. By default, all ports are static-access ports assigned to VLAN 1.
Multi-VLAN	A multi-VLAN port can belong to up to 250 VLANs (some models only support 64 VLANs) and is manually assigned. You cannot configure a multi-VLAN port when a trunk is configured on the switch. VLAN traffic on the multi-VLAN port is not encapsulated.
Trunk (ISL, ATM, or IEEE 802.1Q)	A trunk is a member of all VLANs in the VLAN database by default, but membership can be limited by configuring the allowed-VLAN list. You can also modify the pruning-eligible list to block flooded traffic to VLANs on trunk ports that are included in the list. VLAN Trunking Protocol (VTP) maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP exchanges VLAN configuration messages with other switches over trunk links. **Note** By using the Asynchronous Transfer Mode (ATM) module CLI, you can map the LAN emulation (LANE) client to a VLAN or bind one or more permanent virtual connections (PVCs) to a VLAN. The VLAN ID is then displayed in the Assigned VLANs column of the VLAN Membership window. An ATM port can only be a trunk port. For more information, refer to the *Catalyst 2900 Series XL ATM Modules Installation and Configuration Guide*.
Dynamic access	A dynamic-access port can belong to one VLAN and is dynamically assigned by a VLAN Membership Policy Server (VMPS). The VMPS can be a Catalyst 5000 series switch but never a Catalyst 2900 XL or Catalyst 3500 XL switch.

When a port belongs to a VLAN, the switch learns and manages the addresses associated with the port on a per-VLAN basis. For more information, see the "Managing the MAC Address Tables" section on page 6-15.

VLAN Membership Combinations

You can configure your switch ports in various VLAN membership combinations as listed in Table 8-3.

Table 8-3 VLAN Combinations

Port Mode	VTP Required?	Configuration Procedure	Comments
Static-access ports	No	"Assigning Static-Access Ports to a VLAN" section on page 8-7	If you do not want to use VTP to globally propagate the VLAN configuration information, you can assign a static-access port to a VLAN and set the VTP mode to *transparent* to disable VTP.
Static-access and multi-VLAN ports	No	"Overlapping VLANs and Multi-VLAN Ports" section on page 8-7 "Assigning Static-Access Ports to a VLAN" section on page 8-7	You must connect the multi-VLAN port to a router or server. The switch automatically transitions to VTP transparent mode (VTP is disabled). No VTP configuration is required. Some restrictions apply to multi-VLAN ports. For more information, see the "Avoiding Configuration Conflicts" section on page 9-2.
Static-access and trunk ports	Recommended	"Configuring VTP Server Mode" section on page 8-15 Add, modify, or remove VLANs in the database as described in the "Configuring VLANs in the VTP Database" section on page 8-22 "Assigning Static-Access Ports to a VLAN" section on page 8-24 "Configuring a Trunk Port" section on page 8-27	You can configure at least one trunk port on the switch and make sure that this trunk port is connected to the trunk port of a second switch. Some restrictions apply to trunk ports. For more information, see the "Trunks Interacting with Other Features" section on page 8-26. You can change the VTP version on the switch and enable VTP pruning. You can define the allowed-VLAN list, change the pruning-eligible list, and configure the native VLAN for untagged traffic on the trunk port.
Dynamic-access and trunk ports	Yes	"Configuring Dynamic VLAN Membership" section on page 8-38 "Configuring Dynamic Ports on VMPS Clients" section on page 8-39 "Configuring a Trunk Port" section on page 8-27 so that the VMPS client can receive VTP information from the VMPS	You must connect the dynamic-access port to an end station and not to another switch. Configure the VMPS and the client with the same VTP domain name. You can change the reconfirmation interval and the retry count on the VMPS client switch. You can define the allowed-VLAN list, change the pruning-eligible list, and configure the native VLAN for untagged traffic on the trunk port.

Assigning Static-Access Ports to a VLAN

By default, all ports are static-access ports assigned to the management VLAN, VLAN 1.

You can assign a static-access port to a VLAN without having VTP globally propagate VLAN configuration information (VTP is disabled). Configuring the switch for VTP transparent mode disables VTP.

Beginning in privileged EXEC mode, follow these steps to assign ports for multi-VLAN membership:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port to be added to the VLAN.
Step 3	**switchport mode multi**	Enter the VLAN membership mode for multi-VLAN ports.
Step 4	**switchport multi vlan** *vlan-list*	Assign the port to more than one VLAN. Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs. Configuring a switch port for multi-VLAN mode causes VTP to transition to transparent mode, which disables VTP.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show interface** *interface-id* **switchport**	Verify your entries.

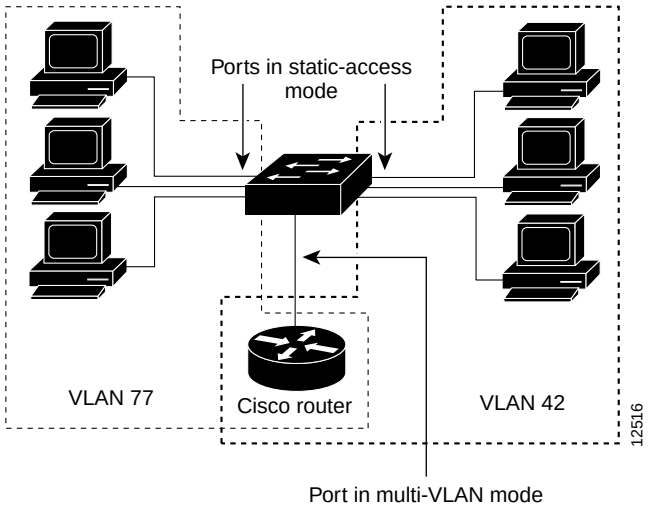
Overlapping VLANs and Multi-VLAN Ports

A multi-VLAN port connected to a router can link two or more VLANs. Intra-VLAN traffic stays within the boundaries of the respective VLANs as shown in Figure 8-2. Connectivity between VLANs is through the router connected to the multi-VLAN port.

A multi-VLAN port performs normal switching functions in all its assigned VLANs. For example, when a multi-VLAN port receives an unknown Media Access Control (MAC) address, all the VLANs to which the port belongs learn the address. Multi-VLAN ports also respond to the STP messages generated by the different instances of STP in each VLAN.

For the restrictions that apply to multi-VLAN ports, see the "Avoiding Configuration Conflicts" section on page 9-2.

Figure 8-2 Two VLANs Sharing a Port Connected to a Router



Caution To avoid unpredictable STP behavior and a loss of connectivity, do not connect multi-VLAN ports to hubs or switches. Connect multi-VLAN ports to routers or servers.

Beginning in privileged EXEC mode, follow these steps to assign ports for multi-VLAN membership:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port to be added to the VLAN.
Step 3	**switchport mode multi**	Enter the VLAN membership mode for multi-VLAN ports.
Step 4	**switchport multi vlan** *vlan-list*	Assign the port to more than one VLAN. Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs. Configuring a switch port for multi-VLAN mode causes VTP to transition to transparent mode, which disables VTP.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show interface** *interface-id* **switchport**	Verify your entries.

Using VTP

VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP minimizes misconfigurations and configuration inconsistencies that can cause several problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.

Before you create VLANs, you must decide whether to use VTP in your network. Using VTP, you can make configuration changes centrally on a single switch, such as a Catalyst 2900 XL or Catalyst 3500 XL switch, and have those changes automatically communicated to all the other switches in the network. Without VTP, you cannot send information about VLANs to other switches.

The VTP Domain

A VTP domain (also called a VLAN management domain) consists of one switch or several interconnected switches under the same administrative responsibility. A switch can be in only one VTP domain. You make global VLAN configuration changes for the domain by using the CLI, Cluster Management software, or SNMP.

By default, a Catalyst 2900 XL or Catalyst 3500 XL switch is in the no-management-domain state until it receives an advertisement for a domain over a trunk link (a link that carries the traffic of multiple VLANs) or until you configure a domain name. The default VTP mode is server mode, but VLAN information is not propagated over the network until a domain name is specified or learned.

If the switch receives a VTP advertisement over a trunk link, it inherits the domain name and configuration revision number. The switch then ignores advertisements with a different domain name or an earlier configuration revision number.

When you make a change to the VLAN configuration on a VTP server, the change is propagated to all switches in the VTP domain. VTP advertisements are sent over all trunk connections, including Inter-Switch Link (ISL), IEEE 802.1Q, IEEE 802.10, and ATM LANE.

If you configure a switch for VTP transparent mode, you can create and modify VLANs, but the changes are not transmitted to other switches in the domain, and they affect only the individual switch.

For domain name and password configuration guidelines, see the "Domain Names" section on page 8-13.

VTP Modes and Mode Transitions

You can configure a supported switch to be in one of the VTP modes listed in Table 8-4.

Table 8-4 VTP Modes

VTP Mode	Description
VTP server	In this mode, you can create, modify, and delete VLANs and specify other configuration parameters (such as VTP version) for the entire VTP domain. VTP servers advertise their VLAN configurations to other switches in the same VTP domain and synchronize their VLAN configurations with other switches based on advertisements received over trunk links. In VTP server mode, VLAN configurations are saved in nonvolatile RAM. VTP server is the default mode.
VTP client	In this mode, a VTP client behaves like a VTP server, but you cannot create, change, or delete VLANs on a VTP client. In VTP client mode, VLAN configurations are saved in nonvolatile RAM.
VTP transparent	In this mode, VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, transparent switches do forward VTP advertisements that they receive from other switches. You can create, modify, and delete VLANs on a switch in VTP transparent mode. In VTP transparent mode, VLAN configurations are saved in nonvolatile RAM, but they are not advertised to other switches.

Two configurations can cause a switch to automatically change its VTP mode:

- When the network is configured with more than the maximum 250 VLANs (some models support a maximum of 64 VLANs), the switch automatically changes from VTP server or client mode to VTP transparent mode. The switch then operates with the VLAN configuration that preceded the one that sent it into transparent mode.
- When a multi-VLAN port is configured on a supported switch in VTP server mode or client mode, the switch automatically changes to transparent mode.

The "VTP Configuration Guidelines" section on page 8-13 provides tips and caveats for configuring VTP.

VTP Advertisements

Each switch in the VTP domain sends periodic global configuration advertisements from each trunk port to a reserved multicast address. Neighboring switches receive these advertisements and update their VTP and VLAN configurations as necessary.

Note Because trunk ports send and receive VTP advertisements, you must ensure that at least one trunk port is configured on the switch and that this trunk port is connected to the trunk port of a second switch. Otherwise, the switch cannot receive any VTP advertisements.

VTP advertisements distribute this global domain information in VTP advertisements:

- VTP domain name
- VTP configuration revision number
- Update identity and update timestamp
- MD5 digest

VTP advertisements distribute this VLAN information for each configured VLAN:

- VLAN ID
- VLAN name
- VLAN type
- VLAN state
- Additional VLAN configuration information specific to the VLAN type

VTP Version 2

VTP version 2 supports these features not supported in version 1:

- Token Ring support—VTP version 2 supports Token Ring LAN switching and VLANs (Token Ring Bridge Relay Function [TRBRF] and Token Ring Concentrator Relay Function [TRCRF]). For more information about Token Ring VLANs, see the "VLANs in the VTP Database" section on page 8-19.
- Unrecognized Type-Length-Value (TLV) support—A VTP server or client propagates configuration changes to its other trunks, even for TLVs it is not able to parse. The unrecognized TLV is saved in nonvolatile RAM when the switch is operating in VTP server mode.
- Version-Dependent Transparent Mode—In VTP version 1, a VTP transparent switch inspects VTP messages for the domain name and version and forwards a message only if the version and domain name match. Because only one domain is supported, VTP version 2 forwards VTP messages in transparent mode without checking the version and domain name.
- Consistency Checks—In VTP version 2, VLAN consistency checks (such as VLAN names and values) are performed only when you enter new information through the CLI, the Cluster Management software, or SNMP. Consistency checks are not performed when new information is obtained from a VTP message or when information is read from nonvolatile RAM. If the digest on a received VTP message is correct, its information is accepted without consistency checks.

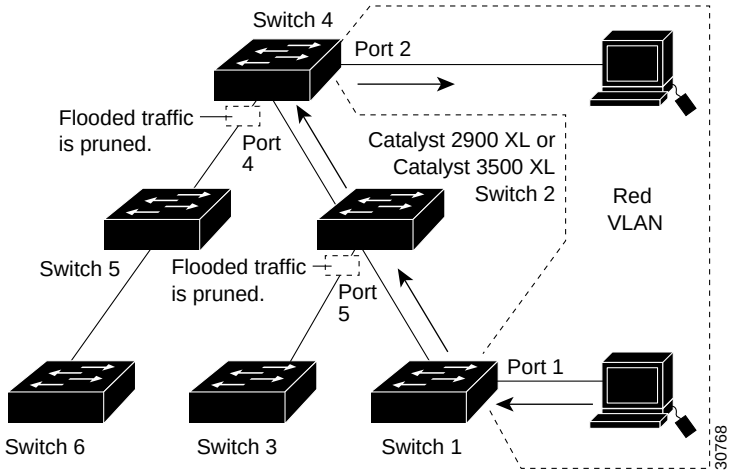
VTP Pruning

Pruning increases available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to reach the destination devices. Without VTP pruning, a switch floods broadcast, multicast, and unknown unicast traffic across all trunk links within a VTP domain even though receiving switches might discard them.

VTP pruning blocks unneeded flooded traffic to VLANs on trunk ports that are included in the pruning-eligible list. Only VLANs included in the pruning-eligible list can be pruned. By default, VLANs 2 through 1001 are pruning eligible on Catalyst 2900 XL and Catalyst 3500 XL trunk ports. If the VLANs are configured as pruning-ineligible, the flooding continues. VTP pruning is also supported with VTP version 1 and version 2.

Figure 8-3 shows a switched network with VTP pruning enabled. The broadcast traffic from Switch 1 is not forwarded to Switches 3, 5, and 6 because traffic for the Red VLAN has been pruned on the links indicated (port 5 on Switch 2 and port 4 on Switch 4).

Figure 8-3 Optimized Flooded Traffic with VTP Pruning



VTP Configuration Guidelines

These sections describe the guidelines you should follow when configuring the VTP domain name and password and the VTP version number.

Domain Names

When configuring VTP for the first time, you must always assign a domain name. All switches in the VTP domain must also be configured with the same domain name. Switches in VTP transparent mode do not exchange VTP messages with other switches, and you do not need to configure a VTP domain name for them.

Caution Do not configure a VTP domain if all switches are operating in VTP client mode. If you configure the domain, it is impossible to make changes to the VLAN configuration of that domain. Therefore, make sure you configure at least one switch in the VTP domain for VTP server mode.

Passwords

You can configure a password for the VTP domain, but it is not required. All domain switches must share the same password. Switches without a password or with the wrong password reject VTP advertisements.

Caution The domain does not function properly if you do not assign the same password to each switch in the domain.

If you configure a VTP password for a domain, a Catalyst 2900 XL or Catalyst 3500 XL switch that is booted without a VTP configuration does not accept VTP advertisements until you configure it with the correct password. After the configuration, the switch accepts the next VTP advertisement that uses the same password and domain name in the advertisement.

If you are adding a new switch to an existing network that has VTP capability, the new switch learns the domain name only after the applicable password has been configured on the switch.

Upgrading from Previous Software Releases

When you upgrade from a software version that supports VLANs but does not support VTP, such as Cisco IOS Release 11.2(8)SA3, to a version that does support VTP, ports that belong to a VLAN retain their VLAN membership, and VTP enters transparent mode. The domain name becomes UPGRADE, and VTP does not propagate the VLAN configuration to other switches.

If you want the switch to propagate VLAN configuration information to other switches and to learn the VLANs enabled on the network, you must configure the switch with the correct domain name, the domain password, and change the VTP mode to VTP server.

VTP Version

Follow these guidelines when deciding which VTP version to implement:

- All switches in a VTP domain must run the same VTP version.
- A VTP version 2-capable switch can operate in the same VTP domain as a switch running VTP version 1 if version 2 is disabled on the version 2-capable switch. Version 2 is disabled by default.
- Do not enable VTP version 2 on a switch unless all of the switches in the same VTP domain are version-2-capable. When you enable version 2 on a switch, all of the version-2-capable switches in the domain enable version 2. If there is a version 1-only switch, it will not exchange VTP information with switches with version 2 enabled.
- If there are Token Ring networks in your environment (TRBRF and TRCRF), you must enable VTP version 2 for Token Ring VLAN switching to function properly. To run Token Ring and Token Ring-Net, disable VTP version 2.
- Enabling or disabling VTP pruning on a VTP server enables or disables VTP pruning for the entire VTP domain.

Default VTP Configuration

Table 8-5 shows the default VTP configuration.

Table 8-5 VTP Default Configuration

Feature	Default Value
VTP domain name	Null.
VTP mode	Server.
VTP version 2 enable state	Version 2 is disabled.
VTP password	None.
VTP pruning	Disabled.

Configuring VTP

You can configure VTP through the CLI by entering commands in the VLAN database command mode. When you enter the **exit** command in VLAN database mode, it applies all the commands that you entered. VTP messages are sent to other switches in the VTP domain, and you enter privileged EXEC mode.

If you are configuring VTP on a cluster member switch to a VLAN, first log in to the member switch by using the privileged EXEC **rcommand** command. For more information on how to use this command, refer to the *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference*.

Note The Cisco IOS **end** and Ctrl-Z commands are not supported in VLAN database mode.

After you configure VTP, you must configure a trunk port so that the switch can send and receive VTP advertisements. For more information, see the "How VLAN Trunks Work" section on page 8-25.

Configuring VTP Server Mode

When a switch is in VTP server mode, you can change the VLAN configuration and have it propagated throughout the network.

Beginning in privileged EXEC mode, follow these steps to configure the switch for VTP server mode:

	Command	Purpose
Step 1	**vlan database**	Enter VLAN database mode.
Step 2	**vtp domain** *domain-name*	Configure a VTP administrative-domain name. The name can be from 1 to 32 characters. All switches operating in VTP server or client mode under the same administrative responsibility must be configured with the same domain name.
Step 3	**vtp password** *password-value*	(Optional) Set a password for the VTP domain. The password can be from 8 to 64 characters. If you configure a VTP password, the VTP domain does not function properly if you do not assign the same password to each switch in the domain.
Step 4	**vtp server**	Configure the switch for VTP server mode (the default).
Step 5	**exit**	Return to privileged EXEC mode.
Step 6	**show vtp status**	Verify the VTP configuration. In the display, check the VTP Operating Mode and the VTP Domain Name fields.

Configuring VTP Client Mode

When a switch is in VTP client mode, you cannot change its VLAN configuration. The client switch receives VTP updates from a VTP server in the VTP domain and then modifies its configuration accordingly.

Caution Do not configure a VTP domain name if all switches are operating in VTP client mode. If you do so, it is impossible to make changes to the VLAN configuration of that domain. Therefore, make sure you configure at least one switch as the VTP server.

Beginning in privileged EXEC mode, follow these steps to configure the switch for VTP client mode:

	Command	Purpose
Step 1	**vlan database**	Enter VLAN database mode.
Step 2	**vtp client**	Configure the switch for VTP client mode. The default setting is VTP server.
Step 3	**vtp domain** *domain-name*	Configure a VTP administrative-domain name. The name can be from 1 to 32 characters. All switches operating in VTP server or client mode under the same administrative responsibility must be configured with the same domain name.
Step 4	**vtp password** *password-value*	(Optional) Set a password for the VTP domain. The password can be from 8 to 64 characters. If you configure a VTP password, the VTP domain does not function properly if you do not assign the same password to each switch in the domain.
Step 5	**exit**	Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode.
Step 6	**show vtp status**	Verify the VTP configuration. In the display, check the VTP Operating Mode field.

Disabling VTP (VTP Transparent Mode)

When you configure the switch for VTP transparent mode, you disable VTP on the switch. The switch then does not send VTP updates and does not act on VTP updates received from other switches. However, a VTP transparent switch does forward received VTP advertisements on all of its trunk links.

Beginning in privileged EXEC mode, follow these steps to configure the switch for VTP transparent mode:

	Command	Purpose
Step 1	**vlan database**	Enter VLAN database mode.
Step 2	**vtp transparent**	Configure the switch for VTP transparent mode. The default setting is VTP server. This step disables VTP on the switch.
Step 3	**exit**	Return to privileged EXEC mode.
Step 4	**show vtp status**	Verify the VTP configuration. In the display, check the VTP Operating Mode field.

Enabling VTP Version 2

VTP version 2 is disabled by default on VTP version 2-capable switches. When you enable VTP version 2 on a switch, every VTP version 2-capable switch in the VTP domain enables version 2.

Caution VTP version 1 and VTP version 2 are not interoperable on switches in the same VTP domain. Every switch in the VTP domain must use the same VTP version. Do not enable VTP version 2 unless every switch in the VTP domain supports version 2.

Note In a Token Ring environment, you must enable VTP version 2 for Token Ring VLAN switching to function properly.

For more information on VTP version configuration guidelines, see the "VTP Version" section on page 8-14.

Beginning in privileged EXEC mode, follow these steps to enable VTP version 2:

	Command	Purpose
Step 1	**vlan database**	Enter VLAN configuration mode.
Step 2	**vtp v2-mode**	Enable VTP version 2 on the switch. VTP version 2 is disabled by default on VTP version 2-capable switches.
Step 3	**exit**	Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode.
Step 4	**show vtp status**	Verify that VTP version 2 is enabled. In the display, check the VTP V2 Mode field.

Disabling VTP Version 2

Beginning in privileged EXEC mode, follow these steps to disable VTP version 2:

	Command	Purpose
Step 1	**vlan database**	Enter VLAN configuration mode.
Step 2	**no vtp v2-mode**	Disable VTP version 2.
Step 3	**exit**	Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode.
Step 4	**show vtp status**	Verify that VTP version 2 is disabled. In the display, check the VTP V2 Mode field.

Enabling VTP Pruning

Pruning increases available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to access the destination devices. You enable VTP pruning on a switch in VTP server mode.

Pruning is supported with VTP version 1 and version 2. If you enable pruning on the VTP server, it is enabled for the entire VTP domain.

Only VLANs included in the pruning-eligible list can be pruned. By default, VLANs 2 through 1001 are pruning eligible on Catalyst 2900 XL and Catalyst 3500 XL trunk ports. For information, see the "Changing the Pruning-Eligible List" section on page 8-29.

Beginning in privileged EXEC mode, follow these steps to enable VTP pruning:

	Command	Purpose
Step 1	**vlan database**	Enter VLAN configuration mode.
Step 2	**vtp pruning**	Enable pruning in the VTP administrative domain. By default, pruning is disabled. You only need to enable pruning on one switch in VTP server mode.
Step 3	**exit**	Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode.
Step 4	**show vtp status**	Verify your entries. In the display, check the VTP Pruning Mode field.

Monitoring VTP

You monitor VTP by displaying its configuration information: the domain name, the current VTP revision, and the number of VLANs. You can also display statistics about the advertisements sent and received by the switch.

Beginning in privileged EXEC mode, follow these steps to monitor VTP activity:

	Command	Purpose
Step 1	**show vtp status**	Display the VTP switch configuration information.
Step 2	**show vtp counters**	Display counters about VTP messages being sent and received.

VLANs in the VTP Database

You can set these parameters when you add a new VLAN to or modify an existing VLAN in the VTP database:

- VLAN ID
- VLAN name
- VLAN type (Ethernet, Fiber Distributed Data Interface [FDDI], FDDI network entity title [NET], TRBRF or TRCRF, Token Ring, Token Ring-Net)
- VLAN state (active or suspended)
- Maximum transmission unit (MTU) for the VLAN
- Security Association Identifier (SAID)
- Bridge identification number for TRBRF VLANs
- Ring number for FDDI and TRCRF VLANs
- Parent VLAN number for TRCRF VLANs
- STP type for TRCRF VLANs
- VLAN number to use when translating from one VLAN type to another

The "Default VLAN Configuration" section on page 8-20 lists the default values and possible ranges for each VLAN media type.

Token Ring VLANs

Although the Catalyst 2900 XL and Catalyst 3500 XL switches do not support Token Ring connections, a remote device such as a Catalyst 5000 series switch with Token Ring connections could be managed from one of the supported switches. Switches running this IOS release advertise information about these Token Ring VLANs when running VTP version 2:

- Token Ring TRBRF VLANs
- Token Ring TRCRF VLANs

For more information on configuring Token Ring VLANs, refer to the *Catalyst 5000 Series Software Configuration Guide*.

VLAN Configuration Guidelines

Follow these guidelines when creating and modifying VLANs in your network:

- A maximum of 250 VLANs can be active on supported switches, but some models only support 64 VLANs. If VTP reports that there are 254 active VLANs, 4 of the active VLANs (1002 to 1005) are reserved for Token Ring and FDDI.
- Before you can create a VLAN, the switch must be in VTP server mode or VTP transparent mode. For information on configuring VTP, see the "Configuring VTP" section on page 8-15.
- Switches running this IOS release do not support Token Ring or FDDI media. The switch does not forward FDDI, FDDI-Net, TRCRF, or TRBRF traffic, but it does propagate the VLAN configuration through VTP.

Default VLAN Configuration

Table 8-6 through Table 8-10 shows the default configuration for the different VLAN media types.

Note Catalyst 2900 XL and Catalyst 3500 XL switches support Ethernet interfaces exclusively. Because FDDI and Token Ring VLANs are not locally supported, you configure FDDI and Token Ring media-specific characteristics only for VTP global advertisements to other switches.

Table 8-6 Ethernet VLAN Defaults and Ranges

Parameter	Default	Range
VLAN ID	1	1–1005
VLAN name	VLAN*xxxx*, where *xxxx* is the VLAN ID	No range
802.10 SAID	100000+VLAN ID	1–4294967294
MTU size	1500	1500–18190
Translational bridge 1	0	0–1005
Translational bridge 2	0	0–1005
VLAN state	active	active, suspend

Table 8-7 FDDI VLAN Defaults and Ranges

Parameter	Default	Range
VLAN ID	1002	1–1005
VLAN name	VLAN*xxxx*, where *xxxx* is the VLAN ID	No range
802.10 SAID	100000+VLAN ID	1–4294967294
MTU size	1500	1500–18190
Ring number	None	1–4095
Parent VLAN	0	0–1005
Translational bridge 1	0	0–1005
Translational bridge 2	0	0–1005
VLAN state	active	active, suspend

Table 8-8 FDDI-Net VLAN Defaults and Ranges

Parameter	Default	Range
VLAN ID	1004	1–1005
VLAN name	VLAN*xxxx*, where *xxxx* is the VLAN ID	No range
802.10 SAID	100000+VLAN ID	1–4294967294
MTU size	1500	1500–18190
Bridge number	0	0–15
STP type	ieee	auto, ibm, ieee
Translational bridge 1	0	0–1005
Translational bridge 2	0	0–1005
VLAN state	active	active, suspend

Table 8-9 Token Ring (TRBRF) VLAN Defaults and Ranges

Parameter	Default	Range
VLAN ID	1005	1–1005
VLAN name	VLAN*xxxx*, where *xxxx* is the VLAN ID	No range
802.10 SAID	100000+VLAN ID	1–4294967294
MTU size	VTPv1 1500; VTPv2 4472	1500–18190
Bridge number	VTPv1 0; VTPv2 user-specified	0–15
STP type	ibm	auto, ibm, ieee
Translational bridge 1	0	0–1005
Translational bridge 2	0	0–1005
VLAN state	active	active, suspend

Table 8-10 Token Ring (TRCRF) VLAN Defaults and Ranges

Parameter	Default	Range
VLAN ID	1003	1–1005
VLAN name	VLAN*xxxx*, where *xxxx* is the VLAN ID	No range
802.10 SAID	100000+VLAN ID	1–4294967294
Ring Number	VTPv1 default 0; VTPv2 user-specified	1–4095
Parent VLAN	VTPv1 default 0; VTPv2 user-specified	0–1005
MTU size	VTPv1 default 1500; VTPv2 default 4472	1500–18190
Translational bridge 1	0	0–1005
Translational bridge 2	0	0–1005
VLAN state	active	active, suspend
Bridge mode	srb	srb, srt
ARE max hops	7	0–13
STE max hops	7	0–13
Backup CRF	disabled	disable; enable

Configuring VLANs in the VTP Database

You use the CLI **vlan database** VLAN database command to add, change, and delete VLANs. In VTP server or transparent mode, commands to add, change, and delete VLANs are written to the file vlan.dat, and you can display them by entering the privileged EXEC **show vlan** command. The vlan.dat file is stored in nonvolatile memory. The vlan.dat file is upgraded automatically, but you cannot return to an earlier version of Cisco IOS after you upgrade to this release.

Caution You can cause inconsistency in the VLAN database if you attempt to manually delete the vlan.dat file. If you want to modify the VLAN configuration or VTP, use the VLAN database commands described in the *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference*.

You use the interface configuration command mode to define the port membership mode and add and remove ports from VLANs. The results of these commands are written to the running-configuration file, and you can display the file by entering the privileged EXEC **show running-config** command.

Note VLANs can be configured to support a number of parameters that are not discussed in detail in this section. For complete information on the commands and parameters that control VLAN configuration, refer to the *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference*.

Adding a VLAN

Each VLAN has a unique, 4-digit ID that can be a number from 1 to 1001. To add a VLAN to the VLAN database, assign a number and name to the VLAN. For the list of default parameters that are assigned when you add a VLAN, see the "Default VLAN Configuration" section on page 8-20.

If you do not specify the VLAN media type, the VLAN is an Ethernet VLAN.

Beginning in privileged EXEC mode, follow these steps to add an Ethernet VLAN:

	Command	Purpose
Step 1	**vlan database**	Enter VLAN database mode.
Step 2	**vlan** *vlan-id* **name** *vlan-name*	Add an Ethernet VLAN by assigning a number to it. If no name is entered for the VLAN, the default is to append the *vlan-id* to the word VLAN. For example, VLAN0004 could be a default VLAN name. If you do not specify the VLAN media type, the VLAN is an Ethernet VLAN.
Step 3	**exit**	Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode.
Step 4	**show vlan name** *vlan-name*	Verify the VLAN configuration.

Modifying a VLAN

Beginning in privileged EXEC mode, follow these steps to modify an Ethernet VLAN:

	Command	Purpose
Step 1	**vlan database**	Enter VLAN configuration mode.
Step 2	**vlan** *vlan-id* **mtu** *mtu-size*	Identify the VLAN, and change the MTU size.
Step 3	**exit**	Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode.
Step 4	**show vlan** *vlan-id*	Verify the VLAN configuration.

Deleting a VLAN from the Database

When you delete a VLAN from a switch that is in VTP server mode, the VLAN is removed from all switches in the VTP domain. When you delete a VLAN from a switch that is in VTP transparent mode, the VLAN is deleted only on that specific switch.

You cannot delete the default VLANs for the different media types: Ethernet VLAN 1 and FDDI or Token Ring VLANs 1002 to 1005.

Caution When you delete a VLAN, any ports assigned to that VLAN become inactive. They remain associated with the VLAN (and thus inactive) until you assign them to a new VLAN.

Beginning in privileged EXEC mode, follow these steps to delete a VLAN on the switch:

	Command	Purpose
Step 1	**vlan database**	Enter VLAN configuration mode.
Step 2	**no vlan** *vlan-id*	Remove the VLAN by using the VLAN ID.
Step 3	**exit**	Update the VLAN database, propagate it throughout the administrative domain, and return to privileged EXEC mode.
Step 4	**show vlan brief**	Verify the VLAN removal.

Assigning Static-Access Ports to a VLAN

By default, all ports are static-access ports assigned to VLAN 1, which is the default management VLAN. If you are assigning a port on a cluster member switch to a VLAN, first log in to the member switch by using the privileged EXEC **rcommand** command. For more information on how to use this command, refer to the *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference*.

Beginning in privileged EXEC mode, follow these steps to assign a port to a VLAN in the VTP database:

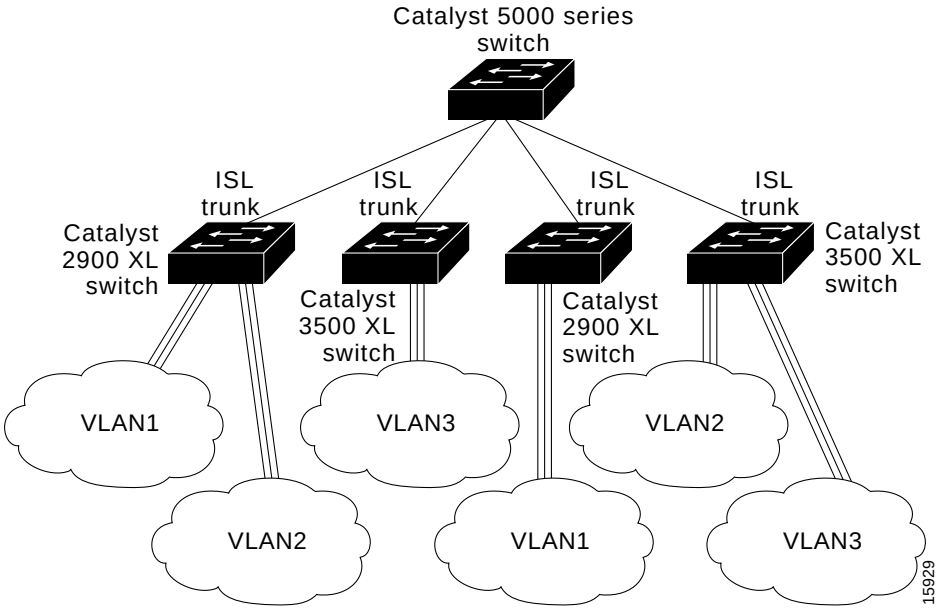
	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and define the interface to be added to the VLAN.
Step 3	**switchport mode access**	Define the VLAN membership mode for this port.
Step 4	**switchport access vlan 3**	Assign the port to the VLAN.
Step 5	**exit**	Return to privileged EXEC mode.
Step 6	**show interface** *interface-id* **switchport**	Verify the VLAN configuration. In the display, check the Operation Mode, Access Mode VLAN, and the Priority for Untagged Frames fields.

How VLAN Trunks Work

A trunk is a point-to-point link that transmits and receives traffic between switches or between switches and routers. Trunks carry the traffic of multiple VLANs and can extend VLANs across an entire network. 100BASE-T and Gigabit Ethernet trunks use Cisco Inter-Switch Link (ISL), the default protocol, or industry-standard IEEE 802.1Q to carry traffic for multiple VLANs over a single link.

Figure 8-4 shows a network of switches that are connected by ISL trunks.

Figure 8-4 Catalyst 2900 XL and Catalyst 3500 XL Switches in an ISL Trunking Environment



IEEE 802.1Q Configuration Considerations

IEEE 802.1Q trunks impose these limitations on the trunking strategy for a network:

- Make sure the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning-tree loops might result.
- Disabling STP on the native VLAN of an 802.1Q trunk without disabling STP on every VLAN in the network can potentially cause STP loops. We recommend that you leave STP enabled on the native VLAN of an 802.1Q trunk or disable STP on every VLAN in the network. Make sure your network is loop-free before disabling STP.

Trunks Interacting with Other Features

ISL, IEEE 802.1Q, and ATM trunking interacts with other switch features as described in Table 8-11.

Table 8-11 Trunks Interacting with Other Features

Switch Feature	Trunk Port Interaction
Port monitoring	A trunk port cannot be a monitor port. A static-access port can monitor the traffic of its VLAN on a trunk port.
Network port	When configured as a network port, a trunk port serves as the network port for all VLANs associated with the port. A network port receives all unknown unicast traffic on a VLAN.
Secure ports	A trunk port cannot be a secure port.
Blocking unicast and multicast packets on a trunk	The **port block** interface configuration command can be used to block the forwarding of unknown unicast and multicast packets to VLANs on a trunk. However, if the trunk port is acting as a network port, unknown unicast packets cannot be blocked.
Port grouping	ISL and 802.1Q trunks can be grouped into EtherChannel port groups, but all trunks in the group must have the same configuration. ATM ports are always trunk ports but cannot be part of an EtherChannel port group. When a group is first created, all ports follow the parameters set for the first port to be added to the group. If you change the configuration of one of these parameters, the switch propagates the setting that you entered to all ports in the group: • Allowed-VLAN list. • STP path cost for each VLAN. • STP port priority for each VLAN. • STP Port Fast setting. • Trunk status: if one port in a port group ceases to be a trunk, all ports cease to be trunks.

Configuring a Trunk Port

You cannot have multi-VLAN and trunk ports configured on the same switch. For information on trunk port interactions with other features, see the "Trunks Interacting with Other Features" section on page 8-26.

Note Because trunk ports send and receive VTP advertisements, you must ensure that at least one trunk port is configured on the switch and that this trunk port is connected to the trunk port of a second switch. Otherwise, the switch cannot receive any VTP advertisements.

Beginning in privileged EXEC mode, follow these steps to configure a port as an ISL or 802.1Q trunk port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface_id*	Enter the interface configuration mode and the port to be configured for trunking.
Step 3	**switchport mode trunk**	Configure the port as a VLAN trunk.
Step 4	**switchport trunk encapsulation** {**isl** | **dot1q**}	Configure the port to support ISL or 802.1Q encapsulation. You must configure each end of the link with the same encapsulation type.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show interface** *interface-id* **switchport**	Verify your entries. In the display, check the Operational Mode and the Operational Trunking Encapsulation fields.
Step 7	**copy running-config startup-config**	Save the configuration.

Note This software release does not support trunk negotiation through the Dynamic Trunking Protocol (DTP), formerly known as Dynamic ISL (DISL). If you are connecting a trunk port to a Catalyst 5000 switch or other DTP device, use the non-negotiate option on the DTP-capable device so that the switch port does not generate DTP frames.

Disabling a Trunk Port

You can disable trunking on a port by returning it to its default static-access mode.

Beginning in privileged EXEC mode, follow these steps to disable trunking on a port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface_id*	Enter the interface configuration mode and the port to be added to the VLAN.
Step 3	**no switchport mode**	Return the port to its default static-access mode.
Step 4	**end**	Return to privileged EXEC.
Step 5	**show interface** *interface-id* **switchport**	Verify your entries. In the display, check the Negotiation of Trunking field.

Defining the Allowed VLANs on a Trunk

By default, a trunk port sends to and receives traffic from all VLANs in the VLAN database. All VLANs, 1 to 1005, are allowed on each trunk. However, you can remove VLANs from the allowed list, preventing traffic from those VLANs from passing over the trunk. To restrict the traffic a trunk carries, use the **remove** *vlan-list* parameter to remove specific VLANs from the allowed list.

A trunk port can become a member of a VLAN if the VLAN is enabled, if VTP knows of the VLAN, and if the VLAN is in the allowed list for the port. When VTP detects a newly enabled VLAN and the VLAN is in the allowed list for a trunk port, the trunk port automatically becomes a member of the enabled VLAN. When VTP detects a new VLAN and the VLAN is not in the allowed list for a trunk port, the trunk port does not become a member of the new VLAN.

Beginning in privileged EXEC mode, follow these steps to modify the allowed list of a ISL or 802.1Q trunk:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface_id*	Enter interface configuration mode and the port to be added to the VLAN.
Step 3	**switchport mode trunk**	Configure VLAN membership mode for trunks.
Step 4	**switchport trunk allowed vlan remove** *vlan-list*	Define the VLANs that are *not* allowed to transmit and receive on the port. The *vlan-list* parameter is a range of VLAN IDs Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs. Valid IDs are from 2 to 1001.
Step 5	**end**	Return to privileged EXEC.
Step 6	**show interface** *interface-id* **switchport allowed-vlan**	Verify your entries.
Step 7	**copy running-config startup-config**	Save the configuration.

Changing the Pruning-Eligible List

The pruning-eligible list applies only to trunk ports. Each trunk port has its own eligibility list. VTP Pruning must be enabled for this procedure to take effect. The "Enabling VTP Pruning" section on page 8-18 describes how to enable VTP pruning.

Beginning in privileged EXEC mode, follow these steps to remove VLANs from the pruning-eligible list on a trunk port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode, and select the trunk port for which VLANs should be pruned.
Step 3	**switchport trunk pruning vlan remove** *vlan-id*	Enter the VLANs to be removed from the pruning-eligible list. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs. Valid IDs are from 2 to 1001. VLANs that are pruning-ineligible receive flooded traffic.
Step 4	**exit**	Return to privileged EXEC mode.
Step 5	**show interface** *interface-id* **switchport**	Verify your settings.

Configuring the Native VLAN for Untagged Traffic

A trunk port configured with 802.1Q tagging can receive both tagged and untagged traffic. By default, the switch forwards untagged traffic with the native VLAN configured for the port. The native VLAN is VLAN 1 by default. For information about 802.1Q configuration issues, see the "IEEE 802.1Q Configuration Considerations" section on page 8-25.

Note The native VLAN can be assigned any VLAN ID, and it is not dependent on the management VLAN.

Beginning in privileged EXEC mode, follow these steps to configure the native VLAN on an 802.1Q trunk:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode, and define the interface that is configured as the 802.1Q trunk.
Step 3	**switchport trunk native vlan** *vlan-id*	Configure the VLAN that is sending and receiving untagged traffic on the trunk port. Valid IDs are from 1 to 1001.
Step 4	**show interface** *interface-id* **switchport**	Verify your settings.

If a packet has a VLAN ID the same as the outgoing port native VLAN ID, the packet is transmitted untagged; otherwise, the switch transmits the packet with a tag.

Configuring 802.1p Class of Service

The Catalyst 2900 XL and Catalyst 3500 XL switches provide quality of service (QoS)-based IEEE 802.1p class of service (CoS) values. QoS uses classification and scheduling to transmit network traffic from the switch in a predictable manner. QoS classifies frames by assigning priority-indexed CoS values to them and gives preference to higher-priority traffic such as telephone calls.

How Class of Service Works

Before you set up 802.1p CoS on a Catalyst 2900 XL or Catalyst 3500 XL switch that operates with the Catalyst 6000 family of switches, refer to the Catalyst 6000 documentation. There are differences in the 802.1p implementation, and they should be understood to ensure compatibility.

Port Priority

Frames received from users in the administratively-defined VLANs are classified or *tagged* for transmission to other devices. Based on rules you define, a unique identifier (the tag) is inserted in each frame header before it is forwarded. The tag is examined and understood by each device before any broadcasts or transmissions to other switches, routers, or end stations. When the frame reaches the last switch or router, the tag is removed before the frame is transmitted to the target end station. VLANs that are assigned on trunk or access ports without identification or a tag are called *native* or *untagged* frames.

For ISL or IEEE 802.1Q frames with tag information, the priority value from the header frame is used. For native frames, the default priority of the input port is used.

Port Scheduling

Each port on the switch has a single receive queue buffer (the *ingress* port) for incoming traffic. When an untagged frame arrives, it is assigned the value of the port as its port default priority. You assign this value by using the CLI or CMS software. A tagged frame continues to use its assigned CoS value when it passes through the ingress port.

CoS configures each transmit port (the *egress* port) with a normal-priority transmit queue and a high-priority transmit queue, depending on the frame tag or the port information. Frames in the normal-priority queue are forwarded only after frames in the high-priority queue are forwarded.

Table 8-12 shows the two categories of switch transmit queues.

Table 8-12 Transmit Queue Information

Transmit Queue Category[1]	Transmit Queues
Catalyst 2900 XL switches, Catalyst 2900 XL Ethernet modules (802.1p user priority)	Frames with a priority value of 0 through 3 are sent to a normal-priority queue. Frames with a priority value of 4 through 7 are sent to a high-priority queue.
Catalyst 3500 XL switches, Gigabit Ethernet modules (802.1p user priority)	Frames with a priority value of 0 through 3 are sent to a normal-priority queue. Frames with a priority value of 4 through 7 are sent to a high-priority queue.

1. Catalyst 2900 XL switches with 4 MB of DRAM and the WS-X2914-XL and the WS-X2922-XL modules only have one transmit queue and do not support QoS.

Configuring the CoS Port Priorities

Beginning in privileged EXEC mode, follow these steps to set the port priority for untagged (native) Ethernet frames:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter the interface to be configured.
Step 3	**switchport priority default** *default-priority-id*	Set the port priority on the interface. If you assign a priority level from 0 to 3, frames are forwarded to the normal priority queue of the output port. If you assign a priority level from 4 to 7, frames are forwarded to the high-priority queue of the output port.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show interface** *interface-id* **switchport**	Verify your entries. In the display, check the Priority for Untagged Frames field.

Load Sharing Using STP

Load sharing divides the bandwidth supplied by parallel trunks connecting switches. To avoid loops, STP normally blocks all but one parallel link between switches. With load sharing, you divide the traffic between the links according to which VLAN the traffic belongs.

You configure load sharing on trunk ports by using STP port priorities or STP path costs. For load sharing using STP port priorities, both load-sharing links must be connected to the same switch. For load sharing using STP path costs, each load-sharing link can be connected to the same switch or to two different switches.

For more information about STP, see the "Configuring STP" section on page 6-33.

Load Sharing Using STP Port Priorities

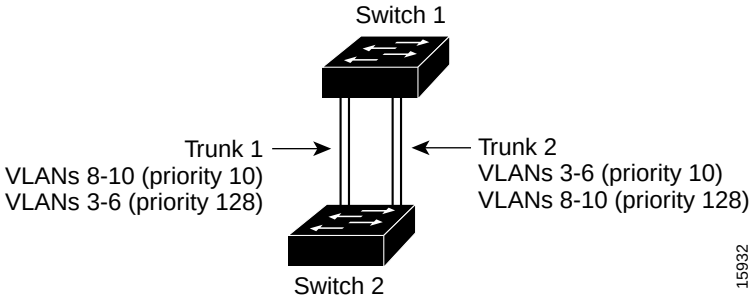
When two ports on the same switch form a loop, the STP port priority setting determines which port is enabled and which port is in standby mode. You can set the priorities on a parallel trunk port so that the port carries all the traffic for a given VLAN. The trunk port with the higher priority (lower values) for a VLAN is forwarding traffic for that VLAN. The trunk port with the lower priority (higher values) for the same VLAN remains in a blocking state for that VLAN. One trunk port transmits or receives all traffic for the VLAN.

Figure 8-5 shows two trunks connecting supported switches. In this example, the switches are configured as follows:

- VLANs 8 through 10 are assigned a port priority of 10 on trunk 1.
- VLANs 3 through 6 retain the default port priority of 128 on trunk 1.
- VLANs 3 through 6 are assigned a port priority of 10 on trunk 2.
- VLANs 8 through 10 retain the default port priority of 128 on trunk 2.

In this way, trunk 1 carries traffic for VLANs 8 through 10, and trunk 2 carries traffic for VLANs 3 through 6. If the active trunk fails, the trunk with the lower priority takes over and carries the traffic for all of the VLANs. No duplication of traffic occurs over any trunk port.

Figure 8-5 Load Sharing by Using STP Port Priorities



Configuring STP Port Priorities and Load Sharing

Beginning in privileged EXEC mode, follow these steps to configure the network shown in Figure 8-5:

	Command	Purpose
Step 1	**vlan database**	On Switch 1, enter VLAN configuration mode.
Step 2	**vtp domain** *domain-name*	Configure a VTP administrative domain. The domain name can be from 1 to 32 characters.
Step 3	**vtp server**	Configure Switch 1 as the VTP server.
Step 4	**exit**	Return to privileged EXEC mode.
Step 5	**show vtp status**	Verify the VTP configuration on both Switch 1 and Switch 2. In the display, check the VTP Operating Mode and the VTP Domain Name fields.
Step 6	**show vlan**	Verify that the VLANs exist in the database on Switch 1.
Step 7	**configure terminal**	Enter global configuration mode.
Step 8	**interface fa0/1**	Enter interface configuration mode, and define Fa0/1 as the interface to be configured as a trunk.
Step 9	**switchport mode trunk**	Configure the port as a trunk port. The trunk defaults to ISL trunking.
Step 10	**end**	Return to privileged EXEC mode.
Step 11	**show interface fa0/1 switchport**	Verify the VLAN configuration.
Step 12		Repeat Steps 7 through 11 on Switch 1 for interface Fa0/2.
Step 13		Repeat Steps 7 through 11 on Switch 2 to configure the trunk ports on interface Fa0/1 and Fa0/2.
Step 14	**show vlan**	When the trunk links come up, VTP passes the VTP and VLAN information to Switch 2. Verify the Switch 2 has learned the VLAN configuration.
Step 15	**configure terminal**	Enter global configuration mode on Switch 1.

	Command	Purpose
Step 16	**interface fa0/1**	Enter interface configuration mode, and define the interface to set the STP port priority.
Step 17	**spanning-tree vlan 8 9 10 port-priority 10**	Assign the port priority of 10 for VLANs 8, 9, and 10.
Step 18	**end**	Return to global configuration mode.
Step 19	**interface fa0/2**	Enter interface configuration mode, and define the interface to set the STP port priority.
Step 20	**spanning-tree vlan 3 4 5 6 port priority 10**	Assign the port priority of 10 for VLANs 3, 4, 5, and 6.
Step 21	**exit**	Return to privileged EXEC mode.
Step 22	**show running-config**	Verify your entries.

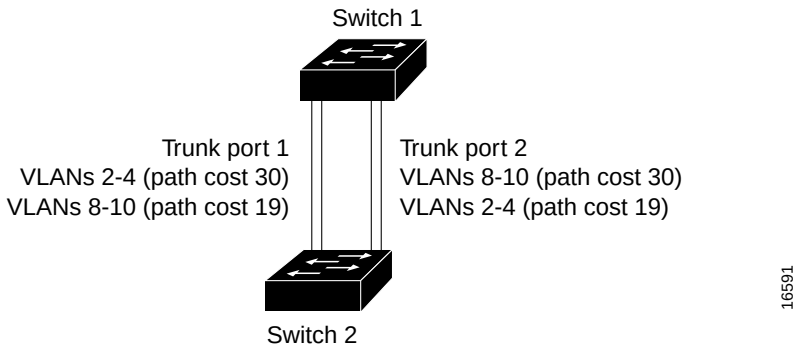
Load Sharing Using STP Path Cost

You can configure parallel trunks to share VLAN traffic by setting different path costs on a trunk and associating the path costs with different sets of VLANs. The VLANs keep the traffic separate; because no loops exist, STP does not disable the ports; and redundancy is maintained in the event of a lost link.

In Figure 8-6, trunk ports 1 and 2 are 100BASE-T ports. The path costs for the VLANs are assigned as follows:

- VLANs 2 through 4 are assigned a path cost of 30 on trunk port 1.
- VLANs 8 through 10 retain the default 100BASE-T path cost on trunk port 1 of 19.
- VLANs 8 through 10 are assigned a path cost of 30 on trunk port 2.
- VLANs 2 through 4 retain the default 100BASE-T path cost on trunk port 2 of 19.

Figure 8-6 Load-Sharing Trunks with Traffic Distributed by Path Cost



Beginning in privileged EXEC mode, follow these steps to configure the network shown in Figure 8-6:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode on Switch 1.
Step 2	**interface fa0/1**	Enter interface configuration mode, and define Fa0/1 as the interface to be configured as a trunk.
Step 3	**switchport mode trunk**	Configure the port as a trunk port. The trunk defaults to ISL trunking.
Step 4	**end**	Return to global configuration mode.
Step 5		Repeat Steps 2 through 4 on Switch 1 interface Fa0/2.
Step 6	**show running-config**	Verify your entries. In the display, make sure that interface Fa0/1 and Fa0/2 are configured as trunk ports.
Step 7	**show vlan**	When the trunk links come up, Switch 1 receives the VTP information from the other switches. Verify that Switch 1 has learned the VLAN configuration.
Step 8	**configure terminal**	Enter global configuration mode.
Step 9	**interface fa0/1**	Enter interface configuration mode, and define Fa0/1 as the interface to set the STP cost.
Step 10	**spanning-tree vlan 2 3 4 cost 30**	Set the spanning-tree path cost to 30 for VLANs 2, 3, and 4.
Step 11	**end**	Return to global configuration mode.
Step 12		Repeat Steps 9 through 11 on Switch 1 interface Fa0/2, and set the spanning-tree path cost to 30 for VLANs 8, 9, and 10.
Step 13	**exit**	Return to privileged EXEC mode.
Step 14	**show running-config**	Verify your entries. In the display, verify that the path costs are set correctly for interface Fa0/1 and Fa0/2.

How the VMPS Works

A switch running this software release acts as a client to the VLAN Membership Policy Server (VMPS) and communicates with it through the VLAN Query Protocol (VQP). When the VMPS receives a VQP request from a client switch, it searches its database for a MAC-address-to-VLAN mapping. The server response is based on this mapping and whether or not the server is in secure mode. Secure mode determines whether the server shuts down the port when a VLAN is not allowed on it or just denies the port access to the VLAN.

In response to a request, the VMPS takes one of these actions:

- If the assigned VLAN is restricted to a group of ports, the VMPS verifies the requesting port against this group and responds as follows:
  - If the VLAN is allowed on the port, the VMPS sends the VLAN name to the client in response.
  - If the VLAN is not allowed on the port, and the VMPS is not in secure mode, the VMPS sends an *access-denied* response.
  - If the VLAN is not allowed on the port, and the VMPS is in secure mode, the VMPS sends *a port-shutdown* response.
- If the VLAN in the database does not match the current VLAN on the port and active hosts exist on the port, the VMPS sends an *access-denied* or a *port-shutdown* response, depending on the secure mode of the VMPS.

If the switch receives an *access-denied* response from the VMPS, it continues to block traffic from the MAC address to or from the port. The switch continues to monitor the packets directed to the port and sends a query to the VMPS when it identifies a new address. If the switch receives a *port-shutdown* response from the VMPS, it disables the port. The port must be manually reenabled by using the CLI, Cluster Management software, or SNMP.

You can also use an explicit entry in the configuration table to deny access to specific MAC addresses for security reasons. If you enter the **none** keyword for the VLAN name, the VMPS sends an *access-denied* or *port-shutdown* response.

Dynamic Port VLAN Membership

A dynamic (nontrunking) port on the switch can belong to only one VLAN. When the link comes up, the switch does not forward traffic to or from this port until the VMPS provides the VLAN assignment. The VMPS receives the source MAC address from the first packet of a new host connected to the dynamic port and attempts to match the MAC address to a VLAN in the VMPS database.

If there is a match, the VMPS sends the VLAN number for that port. If the client switch was not previously configured, it uses the domain name from the first VTP packet it receives on its trunk port from the VMPS. If the client switch was previously configured, it includes its domain name in the query packet to the VMPS to obtain its VLAN number. The VMPS verifies that the domain name in the packet matches its own domain name before accepting the request and responds to the client with the assigned VLAN number for the client.

If there is no match, the VMPS either denies the request or shuts down the port (depending on the VMPS secure mode setting). For more information on possible VMPS responses, see the "How the VMPS Works" section on page 8-35.

Multiple hosts (MAC addresses) can be active on a dynamic port if they are all in the same VLAN; however, the VMPS shuts down a dynamic port if more than 20 hosts are active on the port. If the link goes down on a dynamic port, the port returns to an isolated state and does not belong to a VLAN. Any hosts that come online through the port are checked again with the VMPS before the port is assigned to a VLAN.

VMPS Database Configuration File

The VMPS contains a database configuration file that you create. This ASCII text file is stored on a switch-accessible TFTP server that functions as a VMPS server. The file contains VMPS information, such as the domain name, the fall-back VLAN name, and the MAC address-to-VLAN mapping. A Catalyst 2900 XL or Catalyst 3500 XL switch running this software release cannot act as the VMPS. Use a Catalyst 5000 series switch as the VMPS.

The VMPS database configuration file on the server must use the Catalyst 2900 XL and Catalyst 3500 XL convention for naming ports. For example, Fa0/5 is fixed-port number 5.

If the switch is a cluster member, the command switch adds the name of the switch before the Fa. For example, es3%Fa02 refers to fixed 10/100 port 2 on member switch 3. These naming conventions must be used in the VMPS database configuration file when it is configured to support a cluster.

You can configure a fallback VLAN name. If you connect a device with a MAC address that is not in the database, the VMPS sends the fallback VLAN name to the client. If you do not configure a fallback VLAN and the MAC address does not exist in the database, the VMPS sends an *access-denied* response. If the VMPS is in secure mode, it sends a *port-shutdown* response.

This example shows a sample VMPS database configuration file as it appears on a Catalyst 5000 series switch.

```
!vmps domain <domain-name>
! The VMPS domain must be defined.
!vmps mode { open | secure }
! The default mode is open.
!vmps fallback <vlan-name>
!vmps no-domain-req { allow | deny }
!
! The default value is allow.
vmps domain WBU
vmps mode open
vmps fallback default
vmps no-domain-req deny
!
!
!MAC Addresses
!
vmps-mac-addrs
!
! address <addr> vlan-name <vlan_name>
!
address 0012.2233.4455 vlan-name hardware
address 0000.6509.a080 vlan-name hardware
address aabb.ccdd.eeff vlan-name Green
address 1223.5678.9abc vlan-name ExecStaff
address fedc.ba98.7654 vlan-name --NONE--
address fedc.ba23.1245 vlan-name Purple
!
!Port Groups
!
!vmps-port-group <group-name>
! device <device-id> { port <port-name> | all-ports }
!
vmps-port-group WiringCloset1
 device 192.168.1.1 port Fa1/3
 device 172.16.1.1 port Fa1/4
vmps-port-group “Executive Row”
 device 192.168.2.2 port es5%Fa0/1
 device 192.168.2.2 port es5%Fa0/2
 device 192.168.2.3 all-ports
```

```
!
!VLAN groups
!
!vmps-vlan-group <group-name>
! vlan-name <vlan-name>
!
vmps-vlan-group Engineering
vlan-name hardware
vlan-name software
!
!VLAN port Policies
!
!vmps-port-policies {vlan-name <vlan_name> | vlan-group <group-name> }
! { port-group <group-name> | device <device-id> port <port-name> }
!
vmps-port-policies vlan-group Engineering
 port-group WiringCloset1
vmps-port-policies vlan-name Green
 device 192.168.1.1 port Fa0/9
vmps-port-policies vlan-name Purple
 device 192.168.2.2 port Fa0/10
 port-group “Executive Row”
```

VMPS Configuration Guidelines

These guidelines and restrictions apply to dynamic port VLAN membership:

- You must configure the VMPS before you configure ports as dynamic.
- The communication between a cluster of switches and VMPS is managed by the command switch and includes port-naming conventions that are different from standard port names. For the cluster-based port-naming conventions, see the “VMPS Database Configuration File” section on page 8-36.
- When you configure a port as dynamic, the spanning-tree Port Fast feature is automatically enabled for that port. The Port Fast mode accelerates the process of bringing the port into the forwarding state. You can disable Port Fast mode on a dynamic port.
- Secure ports cannot be dynamic ports. You must disable port security on the port before it becomes dynamic.
- Trunk ports cannot be dynamic ports, but it is possible to enter the **switchport access vlan dynamic** interface configuration command for a trunk port. In this case, the switch retains the setting and applies it if the port is later configured as an access port.

  You must turn off trunking on the port before the dynamic access setting takes effect.
- Dynamic ports cannot be network ports or monitor ports.
- The VTP management domain of the VMPS client and the VMPS server must be the same.

Default VMPS Configuration

Table 8-13 shows the default VMPS and dynamic port configuration on client switches.

Table 8-13 Default VMPS Client and Dynamic Port Configuration

Feature	Default Configuration
VMPS domain server	None
VMPS reconfirm interval	60 minutes
VMPS server retry count	3
Dynamic ports	None configured

Configuring Dynamic VLAN Membership

You must enter the IP address of the Catalyst 5000 switch or the other device acting as the VMPS to configure the Catalyst 2900 XL or Catalyst 3500 XL switch as a client. If the VMPS is being defined for a cluster of switches, enter the address on the command switch.

Beginning in privileged EXEC mode, follow these steps to enter the IP address of the VMPS:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vmps server** *ipaddress* **primary**	Enter the IP address of the switch acting as the primary VMPS server.
Step 3	**vmps server** *ipaddress*	Enter the IP address for the switch acting as a secondary VMPS server. You can enter up to three secondary server addresses.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show vmps**	Verify the VMPS server entry. In the display, check the VMPS Domain Server field.

Configuring Dynamic Ports on VMPS Clients

If you are configuring a port on a member switch as a dynamic port, first log into the member switch by using the privileged EXEC **rcommand** command. For more information on how to use this command, refer to the *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference*.

Caution Dynamic port VLAN membership is for end stations. Connecting dynamic ports to other switches can cause a loss of connectivity.

Beginning in privileged EXEC mode, follow these steps to configure a dynamic port on the VMPS client switches:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode and the switch port that is connected to the end station.
Step 3	**switchport mode access**	Set the port to access mode.
Step 4	**switchport access vlan dynamic**	Configure the port as eligible for dynamic VLAN membership. The dynamic-access port must be connected to an end station.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show interface** *interface* **switchport**	Verify the entry. In the display, check the Operational Mode field.

The switch port that is connected to the VMPS server should be configured as a trunk. For more information, see the "Configuring a Trunk Port" section on page 8-27.

Reconfirming VLAN Memberships

Beginning in privileged EXEC mode, follow these steps to confirm the dynamic port VLAN membership assignments that the switch has received from the VMPS:

	Command	Purpose
Step 1	**vmps reconfirm**	Reconfirm dynamic port VLAN membership.
Step 2	**show vmps**	Verify the dynamic VLAN reconfirmation status.

Changing the Reconfirmation Interval

VMPS clients periodically reconfirm the VLAN membership information received from the VMPS. You can set the number of minutes after which reconfirmation occurs.

If you are configuring a member switch in a cluster, this parameter must be equal to or greater than the reconfirmation setting on the command switch. In addition, you must first log into the member switch by using the privileged EXEC **rcommand** command. For more information about this command, refer to the *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference*.

Beginning in privileged EXEC mode, follow these steps to change the reconfirmation interval:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vmps reconfirm** *minutes*	Enter the number of minutes between reconfirmations of the dynamic VLAN membership. Enter a number from 1 to 120. The default is 60 minutes.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show vmps**	Verify the dynamic VLAN reconfirmation status. In the display, check the Reconfirm Interval field.

Changing the Retry Count

Beginning in privileged EXEC mode, follow these steps to change the number of times that the switch attempts to contact the VMPS before querying the next server:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vmps retry** *count*	Change the retry count. The retry range is from 1 to 10; the default is 3.
Step 3	**exit**	Return to privileged EXEC mode.
Step 4	**show vmps**	Verify your entry. In the display, check the Server Retry Count field.

Administering and Monitoring the VMPS

You can display information about the VMPS by using the privileged EXEC **show vmps** command. The switch displays this information about the VMPS:

VMPS VQP Version	The version of VQP used to communicate with the VMPS. The switch queries the VMPS using version 1 of VQP.
Reconfirm Interval	The number of minutes the switch waits before reconfirming the VLAN-to-MAC-address assignments.
Server Retry Count	The number of times VQP resends a query to the VMPS. If no response is received after this many tries, the switch starts to query the secondary VMPS.
VMPS domain server	The IP address of the configured VLAN membership policy servers. The switch sends queries to the one marked *current*. The one marked *primary* is the primary server.
VMPS Action	The result of the most recent reconfirmation attempt. This can happen automatically when the reconfirmation interval expired, or you can force it by entering the privileged EXEC **vmps reconfirm** command or its Cluster Management software or SNMP equivalent.

Troubleshooting Dynamic Port VLAN Membership

The VMPS shuts down a dynamic port under these conditions:

- The VMPS is in secure mode, and it will not allow the host to connect to the port. The VMPS shuts down the port to prevent the host from connecting to the network.
- More than 20 active hosts reside on a dynamic port.

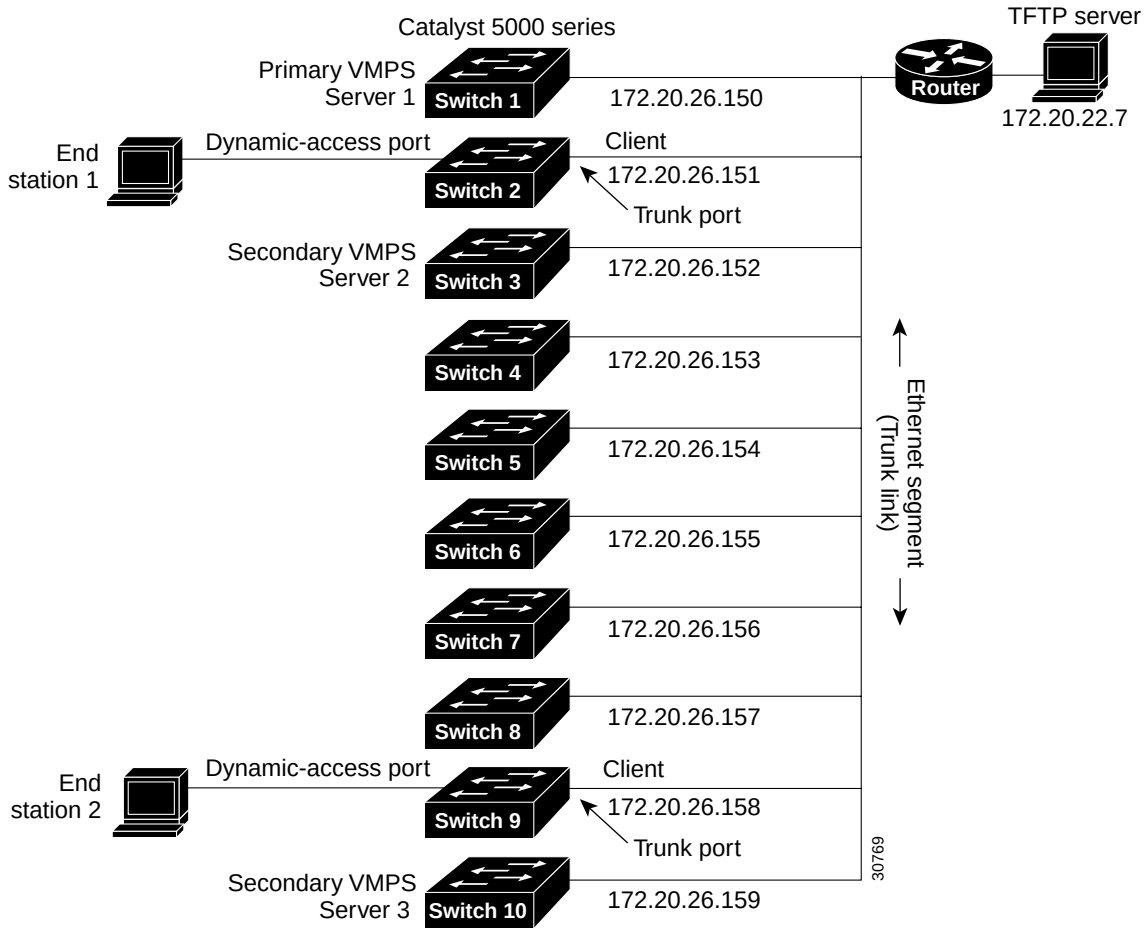
To reenable a shut-down dynamic port, enter the interface configuration **no shutdown** command.

Dynamic Port VLAN Membership Configuration Example

Figure 8-7 shows a network with a VMPS server switch and VMPS client switches with dynamic ports. In this example, these assumptions apply:

- The VMPS server and the VMPS client are separate switches.
- The Catalyst 5000 series Switch 1 is the primary VMPS server.
- The Catalyst 5000 series Switch 3 and Switch 10 are secondary VMPS servers.
- End stations are connected to these clients:
  - Catalyst 2900 XL Switch 2
  - Catalyst 3500 XL Switch 9
- The database configuration file is called Bldg-G.db and is stored on the TFTP server with the IP address 172.20.22.7.

Figure 8-7 Dynamic Port VLAN Membership Configuration



Troubleshooting

This chapter provides these topics about avoiding and resolving problems related to the switch software:

- Avoiding Configuration Conflicts, page 9-2
- Avoiding Autonegotiation Mismatches, page 9-3
- Troubleshooting CMS Sessions, page 9-4
- Determining Why a Switch Is Not Added to a Cluster, page 9-7
- Copying Configuration Files to Troubleshoot Configuration Problems, page 9-8
- Troubleshooting Switch Software Upgrades, page 9-9
- Recovery Procedures, page 9-11

For additional troubleshooting information:

- See Appendix A, “System Messages,” for information about the system messages sent by the switch software.
- Refer to the switch hardware installation guide.

Avoiding Configuration Conflicts

Certain combinations of port features conflict with one another. For example, if you define a port as the network port for a VLAN, all unknown unicast and multicast traffic is flooded to the port. You could not enable port security on the network port because a secure port limits the traffic allowed on it.

In Table 9-1, *no* means that the two features are incompatible and that both should not be enabled; *yes* means that both can be enabled at the same time and will not cause an incompatibility conflict.

If you try to enable incompatible features by using CMS, CMS issues a warning message that you are configuring a setting that is incompatible with another setting, and the switch does not save the change.

Table 9-1 Conflicting Features

	ATM Port[1]	Port Group	Port Security	SPAN Port	Multi-VLAN Port	Network Port	Connect to Cluster?	Protected Port
ATM Port	N/A	No	No	No	No	No	Yes	No
Port Group	No	–	No	No	Yes	Yes[2]	Yes	Yes
Port Security	No	No	–	No	No	No	Yes	Yes
SPAN Port	No[3]	No	No	–	No	No	Yes	Yes
Multi-VLAN Port	No	Yes	No	No	–	Yes	Yes	Yes
Network Port	No	Yes (source-based only)	No	No	Yes	–	No[4]	Yes
Connect to Cluster	Yes	Yes	Yes	Yes	Yes	No	–	Yes
Protected Port	No	Yes	Yes	Yes[5]	Yes	No	Yes	–

1. Catalyst 2900 XL switches only.
2. Cannot be in a destination-based port group.
3. An Asynchronous Transfer Mode (ATM) port cannot be a monitor port but can be monitored.
4. Cannot connect cluster members to the command switch.
5. Switch Port Analyzer (SPAN) can operate only if the monitor port or the port being monitored is not a protected port.

Avoiding Autonegotiation Mismatches

The IEEE 802.3u autonegotiation protocol manages the switch settings for speed (10 Mbps or 100 Mbps) and duplex (half or full). Sometimes this protocol can incorrectly align these settings, reducing performance. A mismatch occurs under these circumstances:

- A manually set speed or duplex parameter is different from the manually set speed or duplex parameter on the connected port.
- A port is set to autonegotiate, and the connected port is set to full duplex with no autonegotiation.

To maximize switch performance and ensure a link, follow one of these guidelines when changing the settings for duplex and speed:

- Let both ports autonegotiate both speed and duplex.
- Manually set the speed and duplex parameters for the ports on both ends of the connection.

Note If a remote Fast Ethernet device does not autonegotiate, configure the duplex settings on the two ports to match. The speed parameter can adjust itself even if the connected port does not autonegotiate. To connect to a remote Gigabit Ethernet device that does not autonegotiate, disable autonegotiation on the local device, and set the duplex and flow control parameters to be compatible with the remote device.

Troubleshooting CMS Sessions

Table 9-2 lists problems commonly encountered when using CMS.

Note

- If your cluster has these member switches running earlier software releases and if you have read-only access to these member switches, some configuration windows for those switches display incomplete information:
  - Catalyst 2900 XL or Catalyst 3500 XL member switches running Cisco IOS Release 12.0(5)WC2 or earlier
  - Catalyst 2950 member switches running Cisco IOS Release 12.0(5)WC2 or earlier
  - Catalyst 3550 member switches running Cisco IOS Release 12.1(6)EA1 or earlier

  For more information about this limitation, refer to the Catalyst 2900 XL and Catalyst 3500 XL release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm).
- These switches do not support read-only mode on CMS:
  - Catalyst 1900 and Catalyst 2820
  - Catalyst 2900 XL switches with 4-MB CPU DRAM

  In read-only mode, these switches appear as unavailable devices and cannot be configured from CMS.

  For more information about CMS access modes, see the "Access Modes in CMS" section on page 2-33.

For more troubleshooting and debugging information while using CMS, you can:

- Use the Java plug-in console to display the current status and actions of CMS. To display the console, select **Start > Programs > Java Plug-in Control Panel**, and select **Java Console**.
- From CMS (**Reports > System Messages**), you can display the system messages of the Catalyst 2900 XL and Catalyst 3500 XL switches when they are in a cluster where the command switch is a Catalyst 2950 switch running Cisco IOS Release 12.1(6)EA2 or later. The System Messages option is not available from the Catalyst 2900 XL and Catalyst 3500 XL switches. For more information about system messages, see Appendix A, "System Messages."

Table 9-2 Common CMS Session Problems

Problem	Suspected Cause and Suggested Solution
A blank screen appears when you click **Cluster Management Suite** from the Cisco Systems Access page.	A missing browser Java plug-in or incorrect settings could cause this problem. • CMS requires a Java plug-in to function correctly. For instructions on downloading and installing the plug-in, refer to the release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm). **Note** If your PC is connected to the Internet when you attempt to access CMS, the browser notifies you that the Java plug-in is required if the plug-in is not installed. This notification does not occur if your PC is directly connected to the switch and has no internet connection. • If the plug-in is installed but the Java applet does not initialize, do this: – Select **Start > Programs > Java Plug-in Control Panel**. In the **Proxies** tab, verify that **Use browser settings** is checked and that no proxies are enabled. – Make sure that the port that connects the PC to the switch belongs to the same VLAN as the management VLAN. For more information about management VLANs, see the "Management VLANs" section on page 8-3.
The **Applet notinited** message appears at the bottom of the browser window.	You might not have enough disk space. Each time you start CMS, the Java plug-in saves a copy of all the jar files to the disk. Delete the jar files from the location where the browser keeps the temporary files on your computer. Refer to the release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm) for the required Java plug-ins.
In an Internet Explorer browser session, you receive a message stating that the CMS page might not display correctly because your security settings prohibit running ActiveX controls.	A high security level prohibits ActiveX controls, which Internet Explorer uses to launch the Java plug-in, from running. 1. Start Internet Explorer. 2. From the menu bar, select **Tools > Internet Options**. 3. Click the **Security** tab. 4. Click the indicated **Zone**. 5. Move the **Security Level for this Zone** slider from **High** to **Medium** (the default). 6. Click **Custom Level** and verify that the four ActiveX settings are set to **prompt** or **enabled**.
Configuration changes are not always reflected in an Internet Explorer 5.0 browser session.	Microsoft Internet Explorer 5.0 does not automatically reflect the latest configuration changes. Make sure you click the browser **Refresh** button for every configuration change.

Table 9-2 Common CMS Session Problems (continued)

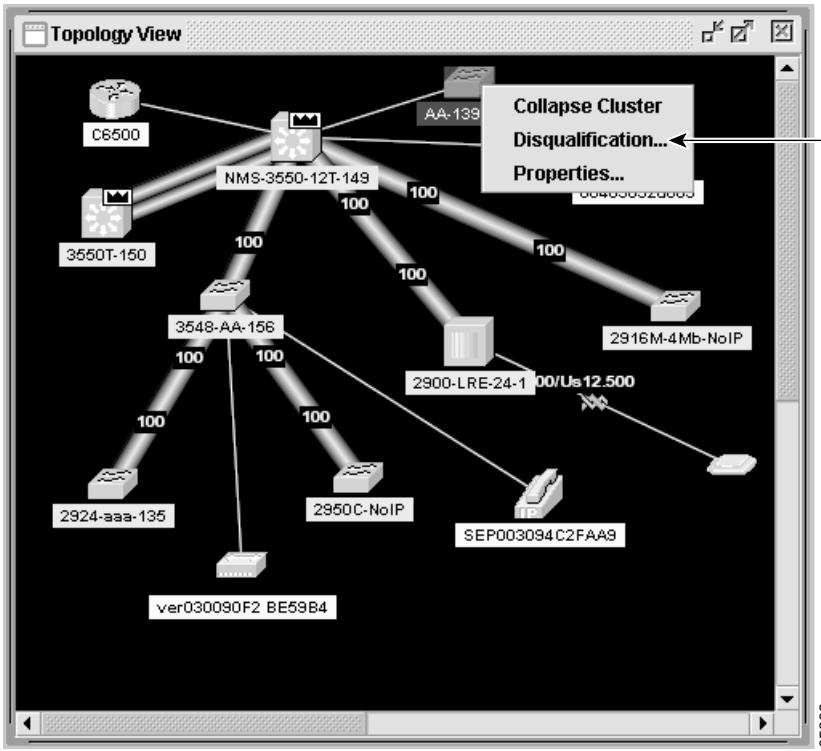
Problem	Suspected Cause and Suggested Solution
Link graphs do not display information in an Internet Explorer 5.0 browser. (For switches running software earlier than Cisco IOS Release 12.0(5)WC3.)	Your browser security settings could be incorrect. If your browser security settings are correct, the lower right corner of your browser screen should have a green circle with a checkmark. If it does not, follow these steps: 1. Start Internet Explorer. 2. From the menu bar, select **Tools > Internet Options**. 3. From the Internet Options window, click **Advanced**. 4. Select the **Java logging enabled** and **JIT compiler for virtual machine enabled** check boxes, and click **Apply**. 5. In the Internet Options window, click **General**. 6. In the Temporary Internet Files section, click **Settings**, click **Every visit to the page**, and click **OK**. 7. In the Internet Options window, click **Security**, click **Trusted Sites**, and click **Sites**. 8. Deselect **Require server verification**. 9. Add the switches you want to manage by entering their URLs in the **Add this web site to the zone** field. Click **Add** to add each switch. A URL is the switch IP address preceded by http://. For example, you might enter: `http://172.20.153.36` 10. After you have finished entering the URLs for your switches, click **OK**. 11. While still in the **Security** tab of the Internet Options window, click **Custom Level**. 12. In the Security Settings window, select **Java > Java permissions**. If you do not see **Java > Java permissions**, you need to reinstall the browser. When you reinstall this browser, make sure to select the **Install Minimal or Customize Your Browser** check box. Then, from the Component Options window in the Internet Explorer 5 section, make sure to click the **Microsoft Virtual Machine** check box to display applets written in Java. 13. Click **Custom**, and click **Java Custom Settings**. 14. In the Trusted Sites window, click **Edit Permissions**. 15. Under **Run Unsigned Content**, click **Enable**, and click **OK**. 16. In the Security Settings window, click **OK**. 17. In the Internet Options window, click **OK**.

Determining Why a Switch Is Not Added to a Cluster

If a switch does not become part of the cluster, you can learn why by selecting **View** > **Topology**. Topology view displays the cluster as a double-switch icon and shows connections to devices outside the cluster (Figure 9-1). Right-click the device (yellow label), and select **Disqualification Code**.

For a list of devices that are cluster-enabled, refer to the release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm).

Figure 9-1 Cluster View



Right-click a device with a yellow label to display the device pop-up menu, and select **Disqualification** to display the reason it could not join the cluster.

Copying Configuration Files to Troubleshoot Configuration Problems

You can use the file system in Flash memory to copy files and to troubleshoot configuration problems. This could be useful if you wanted to save configuration files on an external server in case a switch fails. You can then copy the configuration file to a replacement switch and avoid having to reconfigure the switch.

Step 1 Enter the privileged EXEC **dir flash:** command to display the contents of Flash memory:

```
switch# dir flash:
Directory of flash:

  2  -rwx      843947   Mar 01 1993 00:02:18  C2900XL-h-mz-112.8-SA
  4  drwx        3776   Mar 01 1993 01:23:24  html
 66  -rwx         130   Jan 01 1970 00:01:19  env_vars
 68  -rwx        1296   Mar 01 1993 06:55:51  config.text

1728000 bytes total (456704 bytes free)
```

The file system uses a URL-based file specification. This example uses the TFTP protocol to copy the file config.text from the host *arno* to the switch Flash memory:

```
switch# copy tftp://arno//2900/config.text flash:config.text
```

You can enter these parameters as part of a filename:

- TFTP
- Flash
- RCP
- XMODEM

Step 2 Enter the **copy running-config startup-config** privileged EXEC command to save your configuration changes to Flash memory so that they are not lost if there is a system reload or power outage. This example shows how to use this command to save your changes:

```
switch# copy running-config startup-config
Building configuration...
```

It might take a minute or two to save the configuration to Flash memory. After it has been saved, this message appears:

```
[OK]
switch#
```

Troubleshooting Switch Software Upgrades

Table 9-3 lists problems commonly encountered when upgrading the switch:

Table 9-3 Problems Encountered When Upgrading the Switch

Problem	Suspected Cause and Suggested Solution
Getting "Address Range" error message and boot up is failing.	This error message appears when a 4-MB Catalyst 2900 XL switch is upgraded to an image that is not supported on this hardware. The switch in this case tries to load the image, but because this switch is not capable of loading this image, the bootup process fails. This also happens in cases when a 4-MB Catalyst 2900 XL switch is upgraded to an IOS 12.0 image. Download the IOS Image File by using X-Modem.
Getting "No Such File or Directory" error message during bootup.	This error message appears when the names of the bootable file and the actual file in the Flash memory differ. This usually happens due to a mistyped filename when setting the boot parameters, during or after the upgrade. Go to Setting BOOT Parameters at ROMMON (Switch: Prompt) to verify and set the BOOT parameters correctly. If setting the BOOT parameters to the correct filename does not resolve the issue, perform an X-Modem upgrade, as the file in Flash memory could be corrupted or invalid.
Getting "Permission Denied" error message during the bootup.	This error message appears when the boot parameters are not set correctly. In most of the cases, when setting the boot parameters during or after the upgrade, the word **flash:** is mistyped or completely missed. Go to Setting BOOT Parameters at ROMMON (Switch: Prompt) to verify and set the BOOT parameters correctly. If setting the BOOT parameters to the correct filename does not resolve the issue, perform an X-Modem upgrade, as the file present on the Flash memory could be corrupted or invalid.
Getting "Error Loading Flash" error messages.	The error loading Flash message means that there is a problem loading the current image in Flash memory. The image could be corrupt or incorrect, or the image in Flash memory could be missing. If the system is unable to load a software image in Flash memory, the system will load the boot helper and bring up a switch prompt. 1. Enter the **dir flash:** command to verify if there is any bootable image on the Flash memory. The file with the .bin extension is the bootable image on the Flash memory. If you see a bootable image on the Flash memory, continue to Step 2. If you do not see any bootable image in the Flash memory, download the IOS Image File by using X-Modem. 2. Enter the **set BOOT flash:** *name of IOS file* command to set the boot variable to the filename displayed in Step 1. **Note** BOOT must be capitalized and make sure to include **flash:** before the filename. 3. Enter the **boot** command. **Note** If the switch boots properly, enter the **setting boot parameters** global configuration command to verify and set the BOOT parameters (if needed), and proceed to Step 4. If the switch fails to boot properly, download the IOS Image File by using X-Modem. 4. After setting the BOOT parameters, reload the switch by entering the **reload** privileged EXEC command. The switch boots up automatically with the correct image.

Table 9-3 Problems Encountered When Upgrading the Switch (continued)

Problem	Suspected Cause and Suggested Solution
Failed software upgrade; switch is resetting continuously.	This might be due to a corrupt or incorrect image, or the image in Flash memory might be missing. Following these steps to recover if the switch is in a reset loop after or during the upgrade. 1. Connect the PC to the switch console port. 2. Press the **Enter** key a few times. Are you seeing a *`switch: prompt`*? If not, go to Step 3. Otherwise, go to Step 4. 3. Disconnect the power cord. Hold down the mode button on the front of the switch, and plug the power cord back in. All LEDs above all ports are green. Continue to hold down the mode button until the light above port 1 goes out, and then release the mode button. The prompt should be *switch:*. 4. Download the IOS Image File using X-Modem.
After the upgrade, the switch still boots up with the old image.	This happens when either the BOOT parameters are not correct and the switch is still set to boot from the old image or the upgrade did not go through properly. Verify the BOOT parameters, and correct them if needed. • If the BOOT parameters are correct, download the IOS Image File using TFTP. • If the switch still boots with the old image, download the IOS Image File using X-Modem.
Switch not booting automatically; needs a manual boot at the ROMMON (`switch: prompt`).	The switch boot parameters might be set for manual boot. The switch can be set to boot automatically by following these steps: 1. Use Telnet to access the switch, or connect the PC to the switch console port. 2. Enter the privileged EXEC mode by entering the **enable** command at the `switch> prompt`. 3. Enter the global configuration mode by entering **configure terminal** at the `Switch# prompt`. 4. Enter **no boot manual** to tell the switch to boot automatically. 5. Enter **end** to return to privileged EXEC mode, and save the configuration by entering the **write memory** command. 6. Verify the boot parameters by entering **show boot**. Verify that Manual Boot is set to *no*.

Recovery Procedures

The recovery procedures in this section require that you have physical access to the switch. Recovery procedures include these topics:

- Recovering from Lost Member Connectivity, page 9-11
- Recovering from a Command Switch Failure, page 9-11
- Recovering from a Lost or Forgotten Password, page 9-17
- Recovering from Corrupted Software, page 9-19

Recovering from Lost Member Connectivity

Some configurations can prevent the command switch from maintaining contact with member switches. If you are unable to maintain management contact with a member, and the member switch is forwarding packets normally, check for these port-configuration conflicts:

- Member switches cannot connect to the command switch through a port that is defined as a network port. For information on the network port feature, see the "Enabling a Network Port" section on page 7-6.
- Member switches must connect to the command switch through a port that belongs to the same management VLAN. For more information, see the "Management VLAN" section on page 5-16.
- Member switches connected to the command switch through a secured port can lose connectivity if the port is disabled due to a security violation. Secured ports are described in the "Enabling Port Security" section on page 7-12.

Recovering from a Command Switch Failure

You can prepare for a command switch failure by assigning an IP address to a member switch that is command-capable, making a note of the command-switch password, and cabling your cluster to provide redundant connectivity between all member switches and the replacement command switch. Hot Standby Router Protocol (HSRP) is the preferred method for providing a redundant command switch to a cluster. For more information, see the "HSRP and Standby Command Switches" section on page 5-10 and the "Creating a Cluster Standby Group" section on page 5-21. For a list of command-capable Catalyst desktop switches, see the release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm).

If you have not configured a standby command switch, and your command switch loses power or fails in some other way, management contact with the member switches is lost, and a new command switch must be installed. However, connectivity between switches that are still connected is not affected, and the member switches forward packets as usual. You can manage the members as standalone switches through the console port or, if they have IP addresses, through CMS Device Manager.

These sections describe how to recover if a standby command switch was not available when the command switch failed:

- "Replacing a Failed Command Switch with a Cluster Member" section on page 9-12
- "Replacing a Failed Command Switch with Another Switch" section on page 9-14
- "Recovering from a Failed Command Switch Without Replacing the Command Switch" section on page 9-16

Replacing a Failed Command Switch with a Cluster Member

Follow these steps to replace a failed command switch with a command-capable member of the same cluster:

Step 1 Disconnect the command switch from the member switches, and physically remove it from the cluster.

Step 2 Use a member switch in place of the failed command switch, and duplicate its connections to the cluster members.

Step 3 Start a command-line interface (CLI) session on the new command switch.

You can access the CLI by using the console port or, if an IP address has been assigned to the switch, by using Telnet. For details about using the console port, refer to the switch installation guide.

Step 4 At the switch prompt, change to privileged EXEC mode:

```
Switch> enable
Switch#
```

Step 5 Enter the password of the *failed command switch*.

Step 6 From privileged EXEC mode, enter global configuration mode.

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

Step 7 From global configuration mode, remove previous command-switch information from the switch.

```
Switch(config)# no cluster commander-address
```

Step 8 Return to privileged EXEC mode.

```
Switch(config)# exit
Switch#
```

Step 9 Use the setup program to configure the switch IP information.

This program prompts you for an IP address, subnet mask, default gateway, and password. From privileged EXEC mode, enter **setup**, and press **Return**.

```
Switch# setup
         --- System Configuration Dialog ---
At any point you may enter a question mark '?' for help.
Use Ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Continue with configuration dialog? [yes/no]:
```

Step 10 Enter **Y** at the first prompt.

```
Continue with configuration dialog? [yes/no]: y
```

Step 11 Enter the switch IP address, and press **Return**:

```
Enter IP address: ip_address
```

Step 12 Enter the subnet mask, and press **Return**:

```
Enter IP netmask: ip_netmask
```

Step 13 Enter **Y** at the next prompt to specify a default gateway (router):

```
Would you like to enter a default gateway address? [yes]: y
```

Step 14 Enter the IP address of the default gateway, and press **Return**.

```
IP address of the default gateway: ip_address
```

Step 15 Enter a host name for the switch, and press **Return**.

Note On a command switch, the host name is limited to 28 characters; on a member switch to 31 characters. Do not use *-n*, where n is a number, as the last character in a host name for any switch.

```
Enter a host name: host_name
```

Step 16 Enter the password of the *failed command switch*, and press **Return**.

Note The password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, allows spaces, but ignores leading spaces.

```
Enter enable secret: secret_password
```

Step 17 Enter **Y** to enter a Telnet password:

```
Would you like to configure a Telnet password? [yes] y
```

Note The password can be from 1 to 25 alphanumeric characters, is case sensitive, allows spaces, but ignores leading spaces.

Step 18 Enter the Telnet password, and press **Return**:

```
Enter Telnet password: telnet_password
```

Step 19 **Enter Y to configure the switch as the cluster command switch. Enter N to configure it as a member switch or as a standalone switch.**

Note If you enter **N**, the switch appears as a candidate switch in Cluster Builder. In this case, the message in Step 20 does not appear.

```
Would you like to enable as a cluster command switch? y
```

Step 20 **Assign a name to the cluster, and press Return.**

```
Enter cluster name: cls_name
```

Note The cluster name can be 1 to 31 alphanumeric characters, dashes, or underscores.

Step 21 **The** initial configuration is displayed:

```
The following configuration command script was created:

ip subnet-zero
interface VLAN1
ip address 172.20.153.36 255.255.255.0
ip default-gateway 172.20.153.01
hostname host_name
enable secret 5 $1$M3pS$cXtAlkyR3/6Cn8/
line vty 0 15
password telnet_password
```

```
snmp community private rw
snmp community public ro
cluster enable cls_name

end
```

Step 22 Verify that the information is correct.

- If the information is correct, enter **Y** at the prompt, and press **Return**.
- If the information is not correct, enter **N** at the prompt, press **Return**, and begin again at Step 1.

```
Use this configuration? [yes/no]: y
```

Step 23 Start your browser, and enter the switch IP address that you entered in Step 11.

Step 24 Display the CMS Home page for the switch, and select **Enabled** from the Command Switch drop-down list.

Step 25 Click **Cluster Management Suite** to display CMS.

CMS prompts you to add candidate switches. The password of the failed command switch is still valid for the cluster, and you should enter it when candidate switches are proposed for cluster membership.

Replacing a Failed Command Switch with Another Switch

Follow these steps when you are replacing a failed command switch with a switch that is command-capable but not part of the cluster:

Step 1 Insert the new switch in place of the failed command switch, and duplicate its connections to the cluster members.

Step 2 Start a CLI session on the new command switch.

You can access the CLI by using the console port or, if an IP address has been assigned to the switch, by using Telnet. For details about using the console port, refer to the switch hardware installation guide.

Step 3 At the switch prompt, change to privileged EXEC mode:

```
Switch> enable
Switch#
```

Step 4 Enter the password of the *failed command switch.*

Step 5 Use the setup program to configure the switch IP information.

This program prompts you for an IP address, subnet mask, default gateway, and password. From privileged EXEC mode, enter **setup**, and press **Return**.

```
Switch# setup
         --- System Configuration Dialog ---
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Continue with configuration dialog? [yes/no]:
```

Step 6 Enter **Y** at the first prompt.

```
Continue with configuration dialog? [yes/no]: y
```

Step 7 Enter the switch IP address, and press **Return**:

```
Enter IP address: ip_address
```

Step 8 Enter the subnet mask, and press **Return**:

```
Enter IP netmask: ip_netmask
```

Step 9 Enter **Y** at the next prompt to specify a default gateway (router):

```
Would you like to enter a default gateway address? [yes]: y
```

Step 10 Enter the IP address of the default gateway, and press **Return**.

```
IP address of the default gateway: ip_address
```

Step 11 Enter a host name for the switch, and press **Return**.

Note On a command switch, the host name is limited to 28 characters; on a member switch to 31 characters. Do not use -*n*, where n is a number, as the last character in a host name for any switch.

```
Enter a host name: host_name
```

Step 12 Enter the password of the *failed command switch*, and press **Return**.

Note The password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, allows spaces, but ignores leading spaces.

```
Enter enable secret: secret_password
```

Step 13 Enter **Y** to enter a Telnet password:

```
Would you like to configure a Telnet password? [yes] y
```

Note The password can be from 1 to 25 alphanumeric characters, is case sensitive, allows spaces, but ignores leading spaces.

Step 14 Enter the Telnet password, and press **Return**:

```
Enter Telnet password: telnet_password
```

Step 15 Enter Y to configure the switch as the cluster command switch. Enter N to configure it as a member switch or as a standalone switch.

Note If you enter **N**, the switch appears as a candidate switch in Cluster Builder. In this case, the message in Step 20 does not appear.

```
Would you like to enable as a cluster command switch? y
```

Step 16 Assign a name to the cluster, and press Return.

```
Enter cluster name: cls_name
```

Note The cluster name can be 1 to 31 alphanumeric characters, dashes, or underscores.

Step 17 The initial configuration is displayed:

```
The following configuration command script was created:

ip subnet-zero
interface VLAN1
ip address 172.20.153.36 255.255.255.0
ip default-gateway 172.20.153.01
hostname host_name
enable secret 5 $1$M3pS$cXtAlkyR3/6Cn8/
line vty 0 15
password telnet_password
snmp community private rw
snmp community public ro
cluster enable cls_name

end
```

Step 18 Verify that the information is correct.

- If the information is correct, enter **Y** at the prompt, and press **Return**.
- If the information is not correct, enter **N** at the prompt, press **Return**, and begin again at Step 1.

```
Use this configuration? [yes/no]: y
```

Step 19 Start your browser, and enter the switch IP address that you entered in Step 7.

Step 20 Click **Cluster Management Suite** to display CMS.

It prompts you to add the candidate switches. The password of the failed command switch is still valid for the cluster. Enter it when candidate switches are proposed for cluster membership, and click **OK**.

Recovering from a Failed Command Switch Without Replacing the Command Switch

If a command switch fails and there is no standby command switch configured, member switches continue forwarding among themselves, and they can still be managed through normal standalone means. You can configure member switches through the console-port CLI, and they can be managed through SNMP, HTML, and Telnet after you assign an IP address to them.

The password you enter when you log in to the command switch gives you access to member switches. If the command switch fails and there is no standby command switch, you can use the command-switch password to recover. For more information, see the "Recovering from a Command Switch Failure" section on page 9-11.

Recovering from a Lost or Forgotten Password

Follow the steps in this procedure if you have forgotten or lost the switch password.

Step 1 Connect a terminal or PC with terminal emulation software to the console port. For more information, refer to the switch installation guide.

Note You can configure your switch for Telnet by following the procedure in the "Accessing the CLI" section on page 3-7.

Step 2 Set the line speed on the emulation software to 9600 baud.

Step 3 Unplug the switch power cord.

Step 4 Press the **Mode** button, and at the same time, reconnect the power cord to the switch.

You can release the **Mode** button a second or two after the LED above port 1X goes off. Several lines of information about the software appear, as do instructions:

```
The system has been interrupted prior to initializing the flash file system. The following
commands will initialize the flash file system, and finish loading the operating system
software:

flash_init
load_helper
boot
```

Step 5 Initialize the Flash file system:

```
switch: flash_init
```

Step 6 If you had set the console port speed to anything other than 9600, it has been reset to that particular speed. Change the emulation software line speed to match that of the switch console port.

Step 7 Load any helper files:

```
switch: load_helper
```

Step 8 Display the contents of Flash memory:

```
switch: dir flash:
```

The switch file system is displayed:

```
Directory of flash:

  2  -rwx      843947   Mar 01 1993 00:02:18 C2900XL-h-mz-112.8-SA
  4  drwx        3776   Mar 01 1993 01:23:24  html
 66  -rwx         130   Jan 01 1970 00:01:19  env_vars
 68  -rwx        1296   Mar 01 1993 06:55:51  config.text

1728000 bytes total (456704 bytes free)
```

Step 9 Rename the configuration file to config.text.old.

This file contains the password definition.

```
switch: rename flash:config.text flash:config.text.old
```

Step 10 Boot the system:

```
switch: boot
```

You are prompted to start the setup program. Enter **N** at the prompt:

```
Continue with the configuration dialog? [yes/no]: N
```

Step 11 At the switch prompt, change to privileged EXEC mode:

```
switch> enable
```

Step 12 Rename the configuration file to its original name:

```
switch# rename flash:config.text.old flash:config.text
```

Step 13 Copy the configuration file into memory:

```
switch# copy flash:config.text system:running-config
Source filename [config.text]?
Destination filename [running-config]?
```

Press **Return** in response to the confirmation prompts.

The configuration file is now reloaded, and you can use these normal commands to change the password.

Step 14 Enter global configuration mode:

```
switch# config terminal
```

Step 15 Change the password:

```
switch(config)# enable secret <password>
```

or

```
switch(config)# enable password <password>
```

Step 16 Return to privileged EXEC mode:

```
switch(config)# exit
switch#
```

Step 17 Write the running configuration to the startup configuration file:

```
switch# copy running-config startup-config
```

The new password is now included in the startup configuration.

Recovering from Corrupted Software

Switch software can be corrupted during an upgrade, by downloading the wrong file to the switch, and by deleting the image file. In all these cases, the switch does not pass the power-on self-test (POST), and there is no connectivity.

This procedure uses the XMODEM Protocol to recover from a corrupt or wrong image file. There are many software packages that support the XMODEM protocol, and this procedure is largely dependent on the emulation software you are using.

Step 1 Connect a PC with terminal-emulation software supporting the XMODEM Protocol to the switch console port.

Step 2 Set the line speed on the emulation software to 9600 baud.

Step 3 Unplug the switch power cord.

Step 4 Reconnect the power cord to the switch.

The software image does not load. The switch starts in boot loader mode, which is indicated by the `switch:` prompt.

Step 5 Use the boot loader to enter commands, and start the transfer.

```
switch: copy xmodem: flash:image_filename.bin
```

Step 6 When the XMODEM request appears, use the appropriate command on the terminal-emulation software to start the transfer and to copy the software image to Flash memory.

System Messages

This appendix describes the IOS system messages specific for the switch and contains these sections:

- Overview, page A-1
- How to Read System Messages, page A-2
- Error Message Traceback Reports, page A-4
- Error Message and Recovery Procedures, page A-4

This switch software release is based on Cisco IOS Release 12.0. It has been enhanced to support a set of features for the Catalyst 2900 XL and Catalyst 3500 XL switches. This appendix provides system messages that have been created or changed for these switches. This appendix does not provide Cisco IOS Release 12.0 commands and information already documented in the Cisco IOS Release 12.0 documentation on Cisco.com.

Note From CMS (**Reports > System Messages**), you can display the system messages of the Catalyst 2900 XL and Catalyst 3500 XL switches when they are in a cluster where the command switch is a Catalyst 2950 switch running Cisco IOS Release 12.1(6)EA2 or later or a Catalyst 3550 switch running Cisco IOS Release 12.1(8)EA1 or later. The System Messages option is not available from the Catalyst 2900 XL and Catalyst 3500 XL switches.

Overview

The system software sends IOS system messages to the console (and, optionally, to a logging server on another system) during operation. Not all system messages mean problems with your system. Some messages are purely informational, and others can help diagnose problems with communications lines, internal hardware, or the system software. Each message includes the message itself, an explanation of the problem or condition, and, if available, a recommended course of action.

How to Read System Messages

System messages begin with a percent sign (%) and are structured as follows:

%FACILITY-SUBFACILITY-SEVERITY-MNEMONIC: Message-text

- FACILITY is a code consisting of two or more uppercase letters that indicate the facility to which the message refers. A facility can be a hardware device, a protocol, or a module of the system software. Table A-1 lists the system facility codes.

Table A-1 Facility Codes

Code	Facility	Location
AAAA	TACACS+ authentication, authorization, and accounting security	AAAA Messages, page A-5
CAPITOLA	Internal module	CAPITOLA Messages, page A-7
CDP	Cisco Discovery Protocol	CDP Messages, page A-7
CHASSIS	Chassis	CHASSIS Message, page A-8
CMP	Cluster Membership Protocol module	CMP Messages, page A-8
CPU_NET	CPU network interface	CPU_NET Message, page A-9
ENVIRONMENT	Environment	ENVIRONMENT Messages, page A-9
FRANK	Gigabit Ethernet controller	FRANK Messages, page A-10
GBIC_1000BASET	Cisco GigaStack Gigabit Interface Converter	GBIC_1000BASET Messages, page A-15
GIGASTACK	GigaStack GBIC	GigaStack Messages, page A-16
HW_MEMORY	Hardware memory	HW_MEMORY Messages, page A-17
INTERFACE	Interface API	INTERFACE Messages, page A-18
IP	Internet Protocol	IP Messages, page A-18
MAT	MAC address table	MAT Messages, page A-19
MIRROR	Port monitoring	MIRROR Messages, page A-20
MODULES	Module insertion and extraction	MODULES Messages, page A-20
PERF5_HALT_MSG	PERF5 halt (manufacturing test)	PERF5_HALT_MSG Message, page A-21
PM	Port Manager	PM Messages, page A-22
PMSM	Port Manager state machine	PMSM Messages, page A-24
PORT_SECURITY	Port security	PORT_SECURITY Messages, page A-25
PRUNING	VTP pruning	PRUNING Messages, page A-25
RAC	Router autoconfiguration	RAC Message, page A-29
REGISTORS	Hardware register	REGISTORS Messages, page A-29
RTD	Runtime diagnostic	RTD Messages, page A-30
SNMP	Simple Network Management Protocol	RAC Message, page A-29
SPANTREE	Spanning Tree Protocol	SPANTREE Messages, page A-31
SPANTREE_FAST	STP fast convergence	SPANTREE_FAST Messages, page A-34
STORM_CONTROL	Storm control	STORM_CONTROL Message Messages, page A-35

Table A-1 Facility Codes (continued)

Code	Facility	Location
SW_VLAN	VLAN Manager	SW_VLAN Messages, page A-35
SYS	Operating system	SYS Messages, page A-37
TAC	Terminal Access Controller Access Control System Protocol	TAC Messages, page A-40
TTYDRIVER	Terminal driver	TTYDRIVER Messages, page A-41
VQPCLIENT	Dynamic VLAN VQP client	VQPCLIENT Messages, page A-42
VTP	Virtual Terminal Protocol	VTP Message, page A-45

- SEVERITY is a single-digit code from 0 to 7 that reflects the severity of the condition. The lower the number, the more serious the situation. Table A-2 lists the message severity levels.

Table A-2 Message Severity Levels

Severity Level	Description
0 – emergency	System is unusable.
1 – alert	Immediate action required.
2 – critical	Critical condition.
3 – error	Error condition.
4 – warning	Warning condition.
5 – notification	Normal but significant condition.
6 – informational	Informational message only.
7 – debugging	Message that appears during debugging only.

- MNEMONIC is a code that uniquely identifies the error message.
- Message-text is a text string describing the condition. This portion of the message sometimes contains detailed information about the event, including terminal port numbers, network addresses, or addresses that correspond to locations in the system memory address space. Because the information in these variable fields changes from message to message, it is represented here by short strings enclosed in square brackets ([ ]). A decimal number, for example, is represented as [dec]. Table A-3 lists the variable fields in messages.

Table A-3 Representation of Variable Fields in Messages

Representation	Type of Information
[dec]	Decimal
[char]	Single character
[chars]	Character string
[hex]	Hexadecimal integer
[inet]	Internet address

The following is a sample system message:

%LINK-2-BADVCALL: Interface [chars], undefined entry point

Some error messages also indicate the card and slot reporting the error. These error messages begin with a percent sign (%) and are structured as follows:

Error Message `%CARD-SEVERITY-MSG:SLOT %FACILITY-SEVERITY-MNEMONIC: Message-text`

where:

- CARD is a code that describes the type of card reporting the error.
- MSG is a mnemonic that means that this is a message. It is always shown as MSG.
- SLOT means that the slot number of the card reporting the error. It is shown as SLOT followed by a number. (For example, SLOT5.)

Error Message Traceback Reports

Some messages describe internal errors and contain traceback information. This information is very important and should be included when you report a problem to your technical support representative.

The following sample message includes traceback information:

-Process= "Exec", level= 0, pid= 17

-Traceback= 1A82 1AB4 6378 A072 1054 1860

Error Message and Recovery Procedures

This section lists the switch system messages by facility. Within each facility, the messages are listed by severity levels 0 to 7: 0 is the highest severity level, and 7 is the lowest severity level. Each message is followed by an explanation and a recommended action.

AAAA Messages

This section contains the TACACS+ authentication, authorization, and accounting security error messages.

Error Message `AAAA-3-BADCOMM: Trying config command but should not be.`

Explanation An internal error has occurred.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `AAAA-3-BADREG: Illegal registry call.`

Explanation An internal error has occurred.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `AAAA-3-DLRFORKFAIL: Failed to fork process for [chars].`

Explanation Quite likely, the switch ran out of memory. Other explanations are possible.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `AAAA-3-ILLSGNAME: Illegal server-group name [chars] (type [chars]).`

Explanation The given server-group name is a name that could conflict with internally chosen lists.

Recommended Action Pick a different server-group name.

Error Message `AAAA-3-INTERNAL_ERROR: [chars]`

Explanation This is an internal software error.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `AAAA-3-LISTCREATE: The list [dec] for [chars] is NULL. This should never be.`

Explanation One of the method-lists created at startup was not created. This might cause a reload.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `AAAA-3-NOADMINPROC: [chars]`

Explanation Administrative process has been enabled but somehow could not run.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `AAAA-3-NOREG: [chars] method [dec] has no registry!`

Explanation An internal error has occurred.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `AAAA-3-NOSERV: No name for servergroup in method [chars]`

Explanation An internal error has occurred.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `AAAA-3-NOSG: No server-group passed through parser.`

Explanation An internal error has occurred.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

CAPITOLA Messages

This section contains the Capitola internal module error messages.

Error Message `CAPITOLA_MOD-3-APIBADVALUE:\n[chars]: Bad passed in value [chars] is [dec].`

Explanation Error in initialization of port monitor subsystem.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `CAPITOLA_MOD-3-NULLPTR:\n[chars]: Did not expect NULL pointers.`

Explanation Derived pointers are NULL and could be from bad derivation values.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

CDP Messages

This section contains the Cisco Discovery Protocol error messages.

Error Message `CDP-4-DUPLEX_MISMATCH: Duplex mismatch discovered on [chars] ([chars]), with [chars] [chars] ([chars]).`

Explanation CDP discovered a mismatch of duplex configuration.

Recommended Action Configure the interfaces to the same duplex (full or half).

Error Message `CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on [chars] ([dec]), with [chars] [chars] ([dec]).`

Explanation CDP discovered a mismatch of native-VLAN configurations.

Recommended Action Configure the interfaces to the same native VLAN.

CHASSIS Message

This section contains the chassis error message.

Error Message `CHASSIS-5-BLADE_EXTRACT`

Explanation The message means that the hot-swap switch has been pressed.

Recommended Action Extract the module.

CMP Messages

This section contains the Cluster Membership Protocol error messages.

Error Message `CMP-5-ADD: The Device is added to the cluster (Cluster Name:[chars], CMDR IP Address [inet])`

Explanation The message means that the device is added to the cluster: [chars] is the cluster name, and [inet] is the Internet address of the command switch.

Recommended Action No action is required.

Error Message `CMP-5-MEMBER_CONFIG_UPDATE: Received member configuration from member [dec]`

Explanation This message means that the command switch received a member configuration: [dec] is the member number.

Recommended Action No action is required.

Error Message `CMP-5-REMOVE The Device is removed from the cluster (Cluster Name:[chars])`

Explanation The message means that the device is removed from the cluster: [chars] is the cluster name.

Recommended Action No action is required.

Error Message `CMP-5-MGMT_VLAN_CHNG: The management vlan has been changed to [dec]`

Explanation The management VLAN has been changed.

Recommended Action No action is required.

CPU_NET Message

This section contains the CPU network interface error message.

Error Message `CPU_NET-0-QUEUE_STUCK: The interface between the CPU and the switch has\nbecome stuck. The switch must now reset to clear this condition\n.Retrieval queue [dec].\n`

Explanation The CPU can no longer communicate with the network.

Recommended Action Reload the system.

ENVIRONMENT Messages

This section contains the environment error messages.

Error Message `ENVIRONMENT-2-FAN_FAULT: System Fault: FAN FAULT is detected.`

Explanation This message means that an internal fan fault is detected. This message is available only on the Catalyst 3524-PWR XL switch.

Recommended Action Either check the switch itself, or use the **show env** privileged EXEC command to check if a fan on the switch has failed. The Catalyst 3524-PWR XL switch can operate normally with one failed fan. Replace the switch at your convenience.

Error Message `ENVIRONMENT-2-OVER_TEMP: System Fault:OVER TEMPERATURE condition is detected.`

Explanation This message means that an overtemperature condition is detected. This message is available only on the Catalyst 3524-PWR XL switch.

Recommended Action Use the **show env** command to check if an overtemperature condition exists. If it does:

- Place the switch in an environment that is within 32 to 113°F (0 to 45°C).
- Make sure fan intake and exhaust areas are clear.

If a multiple-fan failure is causing the switch to overheat, replace the switch.

FRANK Messages

This section contains the Gigabit Ethernet controller error messages.

Error Message `FRANK-1-BUFFER_STORE_FAIL: 64B frame storage failure on [chars]`

Explanation When storing 64-B frames, the controller has ignored the buffer congestion warnings and kept storing until a buffer reject. Hence, the port bandwidth allocation limit was increased to allow the last frame to be stored without rejection. In spite of this, the frame storage has failed.

Recommended Action This error prevents a crucial workaround for the controller from executing. This brings down the switch and causes it to reload.

Error Message `FRANK-1-BUFFER_STORE_SET_FAIL: 64B frame storage cap_set failure on [chars].`

Explanation When storing 64-B frames, the controller has ignored the buffer congestion warnings and kept storing until a buffer reject. Hence, the port bandwidth allocation limit needs to be increased to allow the last frame to be stored without rejection. However, the set for the extra allocation value has failed.

Recommended Action This error prevents a crucial workaround for the controller from executing. This brings down the switch and causes it to reload.

Error Message `FRANK-1-DIST_FIFO_POLL_HANDLE: [chars]: Failed to allocate molecule handle`

Explanation A molecule chain is sent by the CPU to the controller driver to read the values of all the distribution FIFO registers for the controller. The memory allocation for this molecule has failed during initialization, and this command cannot be issued to the controller.

Recommended Action This error prevents a crucial workaround for the controller from executing. This brings down the switch and causes it to reload.

Error Message `FRANK-1-INSTANCE_NOT_FOUND: Instance to be removed not found\n`

Explanation The controller instance to be removed was not found in the linked list of instances.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `FRANK-1-MODULE_INVALID: Module inserted in slot [int] is invalid\n`

Explanation The module inserted in the slot does not have a device identification that is a Gigabit Ethernet controller-based module.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `FRANK-1-MODULE_UNKNOWN: Module inserted in slot [int] is of unknown type\n`

Explanation The module inserted in the slot has an unidentified device ID.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `FRANK-1-UNKNOWN_FRAME_NOTIFY_FORMAT: Frame Update Notify = [hex] and Queue Type is [dec] for Queue [dec]\n`

Explanation An unknown frame notify format was found. The queue type and queue number are displayed.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `FRANK-3-ADDR_TBL_ENTRIES_EXCEEDED: \nGig Interface: Out of addr tbl entries \n`

Explanation The Gigabit interface has run out of free address table entries for the address map.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `FRANK-3-BIST_FAILURE: \n[chars] : Bist Failure \n`

Explanation The built-in self-test on the controller port has failed.

Recommended Action The BIST failure on the controller port will cause the controller port to be disabled due to POST failure.

Error Message `FRANK-3-BIST_PHASE_FAILURE: \n[chars] :Bist Phase Failure \n`

Explanation The built-in self-test on the controller port has failed.

Recommended Action The BIST failure on the controller port will cause the controller port to be disabled due to POST failure.

Error Message `FRANK-3-FRAME_INVALID: \nException [hex] Seen on Gig Interface [chars]\n`

Explanation A frame-invalid error was seen on the Gigabit port.

Recommended Action Reboot the switch.

Error Message `FRANK-3-GLOBAL_INIT_FAILED: Global Init Failed\n`

Explanation The global initialization of the controller modules has failed.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `FRANK-3-INIT_FAILED:\ n[chars] Initialization failed [[hex]]\n`

Explanation The controller initialization has failed, and the failure error code is printed.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `FRANK-3-INVALID_FWD_RAM_CFG:\n[chars]: Invalid Fwd Ram Config\n`

Explanation The notify queue space overlaps with the address table space.

Recommended Action The forwarding RAM configuration for the Gigabit port is invalid. Reboot the system.

Error Message `FRANK-3-INVALID_VLAN_DESC: Deleting invalid vlan desc!!\n`

Explanation Attempt to free a VLAN descriptor entry that does not exist from the VLAN table.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `FRANK-3-MAINBOARD_INIT_FAILED: Unable to create Mainboard Process\n`

Explanation The creation of the mainboard process for the controller initialization has failed.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `FRANK-3-MEMORY_INIT_FAILED: \nSlot [dec] Initialization failed:Out of Memory\n`

Explanation Memory initialization for the controller port instance has failed.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `FRANK-3-MODULE_CFG_NOT_FOUND: Module configuration not found\n`

Explanation The configuration for the controller module could not be found.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `FRANK-3-MODULE_INIT_FAILED: Module initialization failed\n`

Explanation The initialization for the controller module failed.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `FRANK-3-MODULE_INSERT_FAIL: Module in slot [dec] bringup failed`

Explanation The module could not be hot-inserted.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `FRANK-3-STATIC_ADDR_NOT_FOUND: \n[chars] :Static Address Not Found`

Explanation A static address entry that needs to be deleted from the static address table was not found in the table.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `FRANK-3-SYSTEM_INFO_FAILURE: Failed to get system configuration information\n`

Explanation The system configuration information for the switch chassis could not be obtained.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `FRANK-3-UNKNOWN_VLAN_EVENT: Unknown vlan event\n`

Explanation A VLAN event that is not recognized by the driver was triggered.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `FRANK-3-VLAN_CAP_FIND_FAILED: Cap Find Failed\n`

Explanation Capitola find on the VLAN membership object for that port has failed.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `FRANK-3-VLAN_DESC_EXCEEDED: Out of vlan desc!!\n`

Explanation There are no unused VLAN descriptors left in the VLAN descriptor table for that VLAN ID.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `FRANK-6-MODULE_INSERTED: Module in slot [dec] is inserted`

Explanation A Gigabit Ethernet controller-based module has been hot-inserted in a slot.

Recommended Action No action is required.

Error Message `FRANK-6-MODULE_REMOVED: Module in slot [dec] was removed`

Explanation The module has been removed from the slot.

Recommended Action No action is required.

GBIC_1000BASET Messages

This section contains the 1000BASE-T Cisco Gigabit Interface Converter (GBIC) error messages.

Error Message `GBIC_1000BASET-6-GBIC_1000BASET_DEFAULT_CONFIG: 1000-BaseT GBIC module is detected in [chars]. Speed and duplex will be autonegotiated`

Explanation 1000-BaseT GBIC modules only support autonegotiation on speed and duplex.

Recommended Action No action is required.

Error Message `GBIC_1000BASET-6-GBIC_1000BASET_NO_CONFIG_DUPLEX: Configuration ignored. 1000-BaseT GBIC modules only support autonegotiation on duplex.`

Explanation 1000-BaseT GBIC modules only support autonegotiation on duplex.

Recommended Action No action is required.

Error Message `GBIC_1000BASET-6-GBIC_1000BASET_NO_CONFIG_NEGOTIATE: Configuration ignored. 1000-BaseT GBIC modules only support autonegotiation.`

Explanation 1000-BaseT GBIC modules only support autonegotiation.

Recommended Action No action is required.

Error Message `GBIC_1000BASET-6-GBIC_1000BASET_NO_CONFIG_SPEED: Configuration ignored. 1000-BaseT GBIC modules only support autonegotiation on speed.`

Explanation 1000-BaseT GBIC modules only support autonegotiation on speed.

Recommended Action No action is required.

GigaStack Messages

This section contains the Cisco GigaStack Gigabit Interface Converter (GBIC) error messages.

Error Message `GIGASTACK-1-NO_LOOP_DETECT: The link neighbor of link [dec] of Gigastack GBIC in [chars] did not respond to the loop detection request. If loop topology is deployed, make sure all switches in the stack are running the latest software.`

Explanation No acknowledgement for GigaStack loop detection request is received from one of the links on a GigaStack GBIC. Either the neighboring switch does not support the GigaStack loop-breaking algorithm, or the link between the two GigaStack GBICs is broken. Under this condition, a GigaStack loop topology is not automatically detected, and the connectivity between switches in the stack could be lost.

Recommended Action If loop topology is used in the GigaStack, make sure that the latest software is running on all switches in the stack. Verify that the GigaStack GBICs involved are functioning.

Error Message `GIGASTACK-3-INIT_FAILURE: Gigastack GBIC in [chars] initialization failed.`

Explanation GigaStack GBIC failed POST.

Recommended Action Remove the GigaStack GBIC, and re-insert it into the GBIC slot.

Error Message `GIGASTACK-6-LOOP_BROKEN`

Explanation A loop formed by GigaStack modules is broken because of link loss. Link 2 of the Master Loop Breaker is re-enabled to replace the broken line.

Recommended Action No action is required.

Error Message `GIGASTACK-6-LOOP_DETECTED`

Explanation A loop has been detected in the GigaStack, and this GigaStack GBIC is selected as the master loop breaker. Link 2 of this GigaStack GBIC is disabled to break the loop.

Recommended Action No action is required.

Error Message `GIGASTACK-6-NO_LOOP_DETECT`

Explanation No acknowledgement for GigaStack loop detection request is received from one of the links on a GigaStack GBIC. Either the neighboring switch does not support the GigaStack loop-breaking algorithm, or the link between the two GigaStack GBICs is broken. Under this condition, a GigaStack loop topology is not automatically detected, and the connectivity between switches in the stack could be lost.

Recommended Action If loop topology is used in the GigaStack, make sure that the latest software is running on all switches in the stack. Verify that the GigaStack GBICs involved are functioning.

Error Message `GIGASTACK-6-LOOP_BROKEN: Link loss is detected in the Gigastack loop\nLink 2 of the Gigastack GBIC in [chars] is re-enabled.`

Explanation A loop formed by GigaStack modules is broken because of link loss. Link 2 of the master loop breaker is re-enabled to replace the broken link

Recommended Action No action is required.

Error Message `GIGASTACK-6-LOOP_DETECTED: Gigastack GBIC in [chars] is selected as Master Loop Breaker. \nLink 2 of the Gigastack GBIC is disabled to break the loop.`

Explanation A loop is detected in the GigaStack, and this GigaStack GBIC is selected as the master loop breaker. Link 2 of this GigaStack GBIC is disabled to break the loop.

Recommended Action No action is required.

HW_MEMORY Messages

This section contains the hardware memory error messages.

Error Message `HW_MEMORY-3-READMEMFAIL: \n[chars]: Failed to read [chars] from ASIC.`

Explanation Failed to read memory from hardware.

Recommended Action If this is happening with all features on the switch, this is a hardware failure. Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `HW_MEMORY-3-WRITEMEMFAIL: \n[chars]: Failed to write [chars] to ASIC.`

Explanation Failed to write memory to hardware.

Recommended Action If this is happening with all features on the switch, this is a hardware failure. Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

INTERFACE Messages

This section contains the interface API error messages.

Error Message `INTERFACE_API-1-NOMORESWIDB: No more SWIDB can be allocated, maximum allowed [dec]`

Explanation No more Interfaces can be created because the maximum number of SWIDB allowed for this platform has been reached.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `INTERFACE_API-4-BADPOINTER: Function [chars] detected an invalid [chars] pointer of [hex], ignoring`

Explanation A software error has occurred, this message is displayed when an invalid pointer is detected.

Recommended Action No action is required.

IP Messages

This section contains the Internet Protocol error messages.

Error Message `IP-5-ACL: [chars]`

Explanation Error occured in IP access checks.

Recommended Action No action is required.

MAT Messages

This section contains the MAC address table error messages.

Error Message `MAT-1-BADFRAME: A bad packet is received on switch port [chars]`

Explanation A packet with either a switch error, a network error, or a wrong port number is received by the address learning process.

Recommended Action If problems persist, copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `MAT-1-NOMEM: Could not allocate memory for [chars] at line [dec] in [chars]`

Explanation System ran out of memory; internal software error.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `MAT-1-SELFADDRRCVD: One of switch's own addresses [enet] is received on module [dec] port [dec]`

Explanation A packet with the source address that is the same as one of the switch's own addresses is received by the address learning process.

Recommended Action Detach end stations connected to the port one at a time to identify the device that generates the packet. If the problem persists, copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `MAT-2-MAXMACCOUNT: Maximum number of MAC addresses ([dec]) has been reached in the address table.`

Explanation The address table can only handle a certain number of MAC addresses.

Recommended Action Reduce the number of MAC addresses in the address table.

Error Message `MAT-2-SECURITYREJECT: Security violation occurred on module [dec] port [dec] caused by MAC address [enet]`

Explanation A packet with an unexpected source address is received on a secure port.

Recommended Action Remove the station with the unexpected MAC address from the secure port, or add the MAC address to the secure address table of the secure port.

MIRROR Messages

This section contains the port monitoring error messages.

Error Message `MIRROR-4-MIRROR_ENABLED: \n[chars]: Mirror bit in MIRROR registered is already enabled.`

Explanation The switch is configuring a different mirror-to port, but mirroring is already enabled.

Recommended Action No action is required.

Error Message `MIRROR-4-MONPORT_MISMATCH: \n[chars]: Monitor port on register [dec] does not match given one [dec].`

Explanation The switch is expecting the same values in terms of monitor ports.

Recommended Action No action is required.

MODULES Messages

This section contains the module insertion and extraction error messages.

Error Message `MODULES-0-CANT_EXTRACT: NOTE: Dynamic module extraction is not supported. The switch must now be reset because the module in slot [dec] was removed.`

Explanation Dynamic module extraction is not supported.

Recommended Action Do not remove modules while the system is running.

Error Message `MODULES-0-CANT_INSERT: NOTE: Dynamic module insertion is not supported. Please execute the 'reload' command to bring the module in slot [dec] on line.`

Explanation Dynamic module insertion is not supported.

Recommended Action Reload the system to bring the module on-line.

Error Message `MODULES-1-MUST_RESET: Transient problem detected with module in slot [dec] which requires reset. Module will be reset and restarted.`

Explanation A port problem is detected on the module. The module is reset and is restarted.

Recommended Action If the module continues to reset and restart, copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `MODULES-3-MAC_TBL_SIZE`

Explanation The dynamic module insertion supports less MAC addresses.

Recommended Action Reboot the system to use the module.

Error Message `MODULES-3-MAC_TBL_SIZE: Inserted module in slot [dec] supports only [dec] MAC addresses. The running system supports [dec] MAC addresses. Please use a module which supports [dec] MAC addresses, or reboot the system to use this module.`

Explanation Dynamic module insertion supports less MAC addresses.

Recommended Action Reboot the system to use the module.

PERF5_HALT_MSG Message

This section contains the PERF5 halt (manufacturing test) error message.

Error Message `PERF5_HALT_MSG-1-PERF5HALTERR: Restarting conversation [dec] [chars]\n [chars] Tx [dec] frames, Rx [dec] frames\n [chars] Tx [dec] frames, Rx [dec] frames\n`

Explanation An halt error causes the Perf5 test to either restart or halt.

Recommended Action Based on the error message, locate the problem, correct it, and rerun the test.

PM Messages

This section contains the Port Manager error messages.

Error Message `PM-2-NOMEM: Not enough memory available for [chars]`

Explanation The Port Manager subsystem could not obtain the memory it needed.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `PM-3-NON_SWITCHABLE_PORT: Non-switchable port:[chars].`

Explanation A **switchport configuration** command is only valid on ports that support hardware packet switching.

Recommended Action Do not attempt to use **switchport** commands on standard routed ports. Check the name of the interface you are configuring against the actual hardware.

Error Message `PM-3-PORT_NOT_SHUTDOWN: [chars].`

Explanation A **switchport configuration** command is only valid on ports that are shut down.

Recommended Action Do not attempt to use **switchport** commands until the port is shut down.

Error Message `PM-3-POWER_INLINE_BAD: [chars] is drawing too much power`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `PM-4-BIT_OUTOFRANGE: bit [dec] is not in the expected range of [dec] to [dec]`

Explanation An invalid request was detected by the bitlist subsystem.

Recommended Action No action is required.

Error Message `PM-4-BIT_OUTOFRANGE: bit [dec] is not in the expected range of [dec] to [dec]`

Explanation An invalid request was detected by the Port Manager.

Recommended Action No action is required.

Error Message `PM-4-BAD_CARD_COOKIE: An invalid card cookie was detected`

Explanation An invalid request was detected by the Port Manager.

Recommended Action No action is required.

Error Message `PM-4-BAD_CARD_SLOT: An invalid card slot ([dec]) was detected`

Explanation An invalid request was detected by the Port Manager.

Recommended Action No action is required.

Error Message `PM-4-BAD_COOKIE: [chars] was detected`

Explanation An invalid request was detected by the Port Manager.

Recommended Action No action is required.

Error Message `PM-4-BAD_PORT_COOKIE: An invalid port cookie was detected`

Explanation An invalid request was detected by the Port Manager.

Recommended Action No action is required.

Error Message `PM-4-BAD_PORT_NUMBER: An invalid port number ([dec]) was detected`

Explanation An invalid request was detected by the Port Manager.

Recommended Action No action is required.

Error Message `PM-4-BAD_VLAN_COOKIE: An invalid vlan cookie was detected`

Explanation An invalid request was detected by the Port Manager.

Recommended Action No action is required.

Error Message `PM-4-BAD_VLAN_ID: An invalid vlan id ([dec]) was detected`

Explanation An invalid request was detected by the Port Manager.

Recommended Action No action is required.

PMSM Messages

This section contains the Port Manager state machine error messages.

Error Message `PMSM-4-BADEVENT: Event '[chars]' is invalid for the current state '[chars]':[chars] [chars]`

Explanation The Port Manager subsystem attempted to post an event to a state machine that is invalid for the current state.

Recommended Action No action is required.

Error Message `PMSM-4-INIT: Internal error while initializing state machine '[chars]', state '[chars]': [chars]`

Explanation An invalid request was detected by the Port Manager.

Recommended Action No action is required.

Error Message `PMSM-4-NOTIDLE: Attempted to stop state machine [chars] [chars] but it is not idle`

Explanation The Port Manager subsystem attempted to stop a state machine that has events pending.

Recommended Action No action is required.

Error Message `PMSM-4-STOPPED: Event '[chars]' ignored because the state machine is stopped: [chars] [chars]`

Explanation The Port Manager subsystem attempted to post an event to a state machine that has already been stopped.

Recommended Action No action is required.

Error Message `PMSM-4-TOOMANY: Event '[chars]' ignored because there are too many pending events:[chars] [chars]`

Explanation The Port Manager subsystem attempted to post an event to a state machine that already has the maximum number of events pending.

Recommended Action No action is required.

Error Message `PMSM-4-UNKNOWN: Event ([dec]) is unknown for the state machine:[chars] [chars]`

Explanation The Port Manager subsystem attempted to post an unknown event to a state machine.

Recommended Action No action is required.

PORT_SECURITY Messages

This section contains the port security error messages.

Error Message `PORT_SECURITY-2-SECURITYREJECT`

Explanation A packet with an unexpected source address is received on a secure port.

Recommended Action Remove the station with the unexpected MAC address from the secure port, or add the MAC address to the secure address table of the secure port.

Error Message `PORT_SECURITY-2-SECURITYREJECT: Security violation occurred on module [dec] port [dec] caused by MAC address [enet]`

Explanation A packet with unexpected source address is received on a secure port.

Recommended Action Remove the station with the unexpected MAC address from the secure port, or add the MAC address to the secure address table of the secure port.

PRUNING Messages

This section contains the VLAN Trunking Protocol (VTP) pruning error messages.

Error Message `PRUNING-1-INVTLV: rx summary in domain [chars] with invalid TLV value: [hex]`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `PRUNING-1-JOININVFSTV: Join rx on trunk [chars]-invalid first vlan: [dec]`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `PRUNING-1-JOININVLEN: Join rx on trunk [chars]-invalid len: [dec] ([dec])`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `PRUNING-1-JOININVLSTV: Join rx on trunk [chars]-invalid last vlan: [dec]`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `PRUNING-3-INVASSOC: Invalid vlan local assoc: [hex] ([chars])`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `PRUNING-3-INVLNKST: Invalid link state:[hex]`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `PRUNING-3-INVPMODE: Invalid pruning mode:[hex]`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `PRUNING-3-INVSPTST: Invalid SPT state: [hex]`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `PRUNING-3-ISDEFAULT: Cannot modify default VLAN id [dec]`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `PRUNING-3-NODOMAIN: Domain [chars]([dec]) not found`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `PRUNING-3-NOTRUNK: Trunk [hex] not found([chars])`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `PRUNING-3-NOVLAN: Vlan [dec] not found ([chars])`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `PRUNING-4-NOBUF: No mbuf to build join`

Explanation No explanation is available at this time.

Recommended Action No action is required.

Error Message `PRUNING-5-JOINDIFFDOMAIN: Domain [chars] not found in rx Join (trunk [hex])`

Explanation No explanation is available at this time.

Recommended Action No action is required.

Error Message `PRUNING-5-JOINDISCARD: rx Join on trunk [hex] when pruning disabled`

Explanation No explanation is available at this time.

Recommended Action No action is required.

Error Message `PRUNING-5-JOINNONAME: No domain name in rx Join (trunk [hex])`

Explanation No explanation is available at this time.

Recommended Action No action is required.

Error Message `PRUNING-5-JOINNOTRUNK: Trunk [hex] not found for rx Join`

Explanation No explanation is available at this time.

Recommended Action No action is required.

Error Message `PRUNING-5-LEARNDOMAIN: Learn domain [chars] from network`

Explanation No explanation is available at this time.

Recommended Action No action is required.

Error Message `PRUNING-6-FSMSTCHG: T[chars],V[dec]:st=[chars],event=[chars],new st=[chars]`

Explanation No explanation is available at this time.

Recommended Action No action is required.

RAC Message

This section contains the router autoconfiguration error message.

Error Message `RAC-3-RACNOIPL: Cannot find lease information for interface [chars]`

Explanation An internal error meaning that DHCP-lease information is missing for the interface.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

REGISTORS Messages

This section contains the hardware register error messages.

Error Message `REGISTORS-3-ERRONREAD: [chars]: Failed to read [chars] register.`

Explanation Failed to read a register.

Recommended Action If this is happening with all features on the switch, this is a hardware failure. Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `REGISTORS-3-ERRONWRITE: [chars]: Failed to write [chars] register.`

Explanation Failed to write a register.

Recommended Action If this is happening with all features on the switch, this is a hardware failure. Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

RTD Messages

This section contains the runtime diagnostic error messages.

Error Message `RTD-1-ADDR_FLAP [chars] relearning [dec] addrs per min`

Explanation Normally, MAC addresses are learned once on a port. Occasionally, when a switched network reconfigures, due to either manual or STP reconfiguration, addresses learned on one port are relearned on a different port. However, if there is a port anywhere in the switched domain that is looped back to itself, addresses will jump back and forth between the real port and the port that is in the path to the looped back port. In this message, [chars] is the interface, and [dec] is the number of addresses being learnt.

Recommended Action Determine the real path (port) to the MAC address. Use the **debug ethernet-controller addr** command to see the alternate path-port on which the address is being learned. Go to the switch attached to that port. Note that the **show cdp neighbors** command is useful in determining the next switch. Repeat this procedure until the port is found that is receiving what it is transmitting, and remove that port from the network.

Error Message `RTD-1-LINK_FLAP [chars] link down/up [dec] times per min`

Explanation An excessive number of link down-up events has been noticed on this interface: [chars] is the interface, and [dec] is the number of times that the link goes up and down. This might be the result of reconfiguring the port, or it might mean a faulty device at the other end of the connection.

Recommended Action If someone is reconfiguring the interface or device at the other side of the interface, ignore this message. However, if no one is manipulating the interface or device at the other end of the interface, it is likely that the Ethernet transceiver at one end of the link is faulty and should be replaced.

Error Message `RTD-1-DEAD_PHY: The PHY on [chars] is dead`

Explanation The runtime diagnostic code is no longer able to communicate with the PHY for this interface. This is most likely due to an electrostatic discharge (ESD) event.

Recommended Action Process a return materials authorization (RMA) for the switch or module that contains the malfunctioning ports.

SNMP Messages

This section contains the Simple Network Management Protocol error messages.

Error Message `SNMP-4-NOENGINEID: Remote snmpEngineID for [IP_address] not found when creating user:[chars]`

Explanation An attempt to create a user failed. This is probably because the engine ID of the remote agent (or SNMP manager) was not configured.

Recommended Action No action is required.

SPANTREE Messages

This section contains the Spanning Tree Protocol error messages.

Error Message `SPANTREE-2-BLOCK_PORT_TYPE: Blocking [chars] on vlan [dec]. Inconsistent port type.`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `SPANTREE-2-BLOCK_PVID_LOCAL: Blocking [chars] on vlan [dec]. Inconsistent local vlan.`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `SPANTREE-2-BLOCK_PVID_PEER: Blocking [chars] on vlan [dec]. Inconsistent peer vlan.`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `SPANTREE-3-PORT_SELF_LOOPED: [chars] disabled.`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `SPANTREE-2-RECV_1Q_NON_1QTRUNK: Received 802.1Q BPDU on non 802.1Q trunk [chars] on vlan [dec].`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `SPANTREE-2-RECV_1Q_NON_TRUNK: Received 802.1Q BPDU on non trunk [chars] on vlan [dec].`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `SPANTREE-2-RECV_BAD_TLV: Received SSTP BPDU with bad TLV on [chars] on vlan [dec].`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer vlan id [dec] on [chars] on vlan [dec].`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `SPANTREE-2-ROOTGUARD_BLOCK: Rootguard blocking port [chars] VLAN [dec].`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `SPANTREE-2-ROOTGUARD_CONFIG_CHANGE: Rootguard [chars] on port [chars] VLAN [dec].`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `SPANTREE-2-ROOTGUARD_UNBLOCK: Rootguard unblocking port [chars] VLAN [dec].`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking [chars] on vlan [dec]. Port consistency restored.`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

SPANTREE_FAST Messages

This section contains the Spanning Tree Protocol fast convergence error messages.

Error Message `SPANTREE_FAST-6-PORT_FWD_UPLINK: Port [chars] in vlan [dec] moved to Forwarding (UplinkFast).`

Explanation No explanation is available at this time.

Recommended Action No action is required.

Error Message `SPANTREE_FAST-6-RECD_INF_BPDU: Received inferior BPDU on port [chars] in [chars].`

Explanation No explanation is available at this time.

Recommended Action No action is required.

Error Message `SPANTREE_FAST-6-RECD_RLQ_REPLY: Received RLQ response PDU on port [chars] in [chars].`

Explanation No explanation is available at this time.

Recommended Action No action is required.

Error Message `SPANTREE_FAST-6-RECD_RLQ_REQ: Received RLQ request PDU on port [chars] in [chars].`

Explanation No explanation is available at this time.

Recommended Action No action is required.

STORM_CONTROL Message Messages

This section contains the storm control error message.

Error Message `STORM_CONTROL-2-SHUTDOWN`

Explanation Excessive traffic has been detected on a port that has been configured to be shut down if a storm event is detected.

Recommended Action When the source of the packet storm has been corrected, re-enable the port by using the port-configuration commands.

SW_VLAN Messages

This section contains the VLAN Manager error messages.

Error Message `SW_VLAN-3-VTP_PROTOCOL_ERROR: VTP protocol code internal error:[chars]`

Explanation VLAN Trunking Protocol (VTP) protocol code encountered an unexpected error when processing a configuration request, packet, or timer expiration.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `SW_VLAN-4-BAD_PM_VLAN_COOKIE_RETURNED: VLAN manager unexpectedly received a bad PM VLAN cookie from the Port Manager, VLAN indicated:[dec]`

Explanation The VLAN manager received an upcall from the Port Manager containing a VLAN cookie that translated to a bad VLAN number.

Recommended Action No action is required.

Error Message `SW_VLAN-4-BAD_VLAN_CONFIGURATION_FILE: VLAN configuration file contained incorrect verification word:[hex]`

Explanation The VLAN configuration file read by the VLAN manager did not begin with a correct value that would indicate a valid VLAN configuration file. It has been rejected.

Recommended Action No action is required.

Error Message `SW_VLAN-4-BAD_VLAN_CONFIGURATION_FILE_VERSION: VLAN configuration file contained unknown file version:[dec]`

Explanation The VLAN configuration file read by the VLAN manager contained an unrecognized file version number. (This might mean an attempt to regress to an older version of the VLAN manager software.)

Recommended Action No action is required.

Error Message `SW_VLAN-4-BAD_VLAN_TIMER_ACTIVE_VALUE: Encountered incorrect VLAN timer active value:[chars]`

Explanation Due to a software error, a VLAN timer was detected as active when it should have been inactive or inactive when it should have been active.

Recommended Action No action is required.

Error Message `SW_VLAN-4-IFS_FAILURE: VLAN manager encountered file operation error:call = [chars] / failure code (errno) = [dec] / bytes transfered = [dec]`

Explanation The VLAN manager received an unexpected error return from a IOS file system call.

Recommended Action No action is required.

Error Message `SW_VLAN-4-NO_PM_COOKIE_RETURNED: VLAN manager unexpectedly received a null [chars] type cookie from the Port Manager, data reference:[chars]`

Explanation The VLAN manager queried the Port Manager for a reference cookie but received a NULL pointer instead.

Recommended Action No action is required.

Error Message `SW_VLAN-4-VTP_INTERNAL_ERROR: VLAN manager received an internal error [dec] from vtp function [chars]:[chars]`

Explanation An unexpected error code was received by the VLAN Manager from the VTP configuration software.

Recommended Action No action is required.

Error Message `SW_VLAN-4-VTP_INVALID_DATABASE_DATA: VLAN manager received bad data of type [chars]:value [dec] from vtp database function [chars]`

Explanation Invalid data was received by the VLAN Manager from a VTP configuration database routine.

Recommended Action No action is required.

Error Message `SW_VLAN-4-VTP_INVALID_EVENT_DATA: VLAN manager received bad data of type [chars]:value [dec] while being called to handle a [chars] event`

Explanation Invalid data was received by the VLAN Manager from the VTP configuration software.

Recommended Action No action is required.

Error Message `SW_VLAN-6-OLD_CONFIG_FILE_READ: Old version [dec] VLAN configuration file detected and read OK. Version [dec] files will be written in the future.`

Explanation The VLAN software detected an old version of the VLAN configuration file format. It was able to interpret the file with no problems but will create files using the new format in the future.

Recommended Action No action is required.

Error Message `SW_VLAN-6-VTP_MODE_CHANGE: VLAN manager changing device mode from [chars] to [chars].`

Explanation Some switch devices must automatically change VTP device modes upon receipt of a VLAN configuration database containing more than a set number of VLANs, depending on the device. This message means that such a spontaneous conversion has occurred, what the previous mode was, and what the current mode is.

Recommended Action No action is required.

SYS Messages

This section contains the operating system error messages.

Error Message `SYS-2-CHUNKBADELESIZE: Chunk element size is more than 64k for [chars]`

Explanation Chunk manager cannot function properly with big chunk elements.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `SYS-2-CHUNKBADPOOLSIZE: Bad poolsize returned by the system :[int]`

Explanation The system returns a non-optimal pool size. You need to change pool sizes.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `SYS-2-CHUNKBOUNDSIB: Error noticed in the sibling of the chunk [chars]Chunk index :[dec], Chunk real max :[dec]`

Explanation A software error occurred.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `SYS-2-CHUNKEXPANDFAIL: Could not expand chunk pool for [chars]. No memory available`

Explanation There is not enough processor memory left to increase this chunk pool.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `SYS-2-CHUNKINCONSIS: Inconsistant counters for chunk :[chars]total free [dec]/[dec], total sibs [dec]/[dec], total alloc [dec]/[dec]`

Explanation The system returns a non-optimal pool size. You need to change pool sizes.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `SYS-2-EXCEPTIONDUMP: System Crashed, Writing Core....`

Explanation The system has crashed because of an exception. A core is being generated.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `SYS-2-INLIST1: Buffer in list, ptr= [hex], caller= [hex]`

Explanation An internal software error occurred.

Recommended Action If this messages recurs, copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `SYS-2-SHARED1: Attempt to return buffer with sharecount [dec], ptr= [hex], caller= [hex]`

Explanation An internal software error occurred.

Recommended Action If this messages recurs, copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `SYS-3-BAD_RESET: Questionable reset of process [dec] on tty[t-line]\n`

Explanation A process was reset without giving it a chance to clean itself up.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `SYS-3-DUP_TIMER: Same tty[t-line] in linewatch_timers, type [dec]`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `SYS-3-LOGGER_FLUSHED: System was paused for [time-stamp] to ensure console debugging output.`

Explanation Debugging or informational messages are being generated faster than they can be displayed on the console. To guarantee that they can be seen, the rest of the system was paused until the console output catches up. This can break time-critical behavior, such as maintaining an ISDN link.

Recommended Action Consider using conditional debugging, turning off console logging, using the **no logging console guaranteed** command, or turning off link-state messages for some interfaces.

Error Message `SYS-3-LOGGER_FLUSHING: System pausing to ensure console debugging output.`

Explanation Debugging or informational messages are being generated faster than they can be displayed on the console. To guarantee that they can be seen, the rest of the system is paused until the console output catches up. This can break time-critical behavior, such as maintaining an ISDN link.

Recommended Action Consider using conditional debugging, turning off console logging, using the **no logging console guaranteed** command, or turning off link-state messages for some interfaces.

Error Message `SYS-6-READ_BOOTFILE_FAIL: [chars] [chars].`

Explanation A configured boot system command failed.

Recommended Action If a system image was eventually loaded, no action is required. If the system image did not load as configured, copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

TAC Messages

This section contains the Terminal Access Controller Access Control System Protocol error messages.

Error Message `TAC-3-PICKCTX: No pick-context`

Explanation The context to pick the next server has disappeared.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `TAC-3-XTACACL: [chars]: accesslist [hex] out of range for "[chars]"`

Explanation The TACACS facility created a message that contains an access list that is not a valid access list (out of bounds).

Recommended Action If this message recurs, copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information..

Error Message `TAC-4-NOTIMEOUT: Warning: This command has been deprecated in favor of the line-command "timeout login response"`

Explanation This command is deprecated and should no longer be used. The line **timeout login response** command now provides this functionality.

Recommended Action Use the line command **timeout login response**.

Error Message `TAC-4-UNEXREP: Reply for non-existent request, [dec] on queue`

Explanation The TACACS facility received a message it was not expecting. This might occur when a TACACS server sends duplicate responses or when it responds to a request that has already timed out. It also might be due to an internal software problem.

Recommended Action No action is required.

Error Message `TAC-6-SENDTMO: Send type [dec] to [IP_address] timed out`

Explanation A background TACACS notification (enabled with the **tacacs notify** command) was not acknowledged by the TACACS server processor within the timeout period (5 minutes). The information in that notification was lost. This loss of information might interfere with accounting or auditing on the server. This condition arises when the TACACS server is misconfigured, halted, or became unreachable through the network.

Recommended Action Check the TACACS server and the network attached to it.

TTYDRIVER Messages

This section contains the terminal driver error messages.

Error Message `TTYDRIVER-2-NOBRKPAK: Unable to allocate break block from I/O mem`

Explanation The router does not have enough I/O memory for buffers.

Recommended Action Consider adding more shared memory. Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `TTYDRIVER-2-NOBUFPOOL_ASYNC: Unable to create buffer pool for async. mode interface`

Explanation There is not enough memory for a per-channel control block of the async TTY driver.

Recommended Action Reduce other system activity to ease memory demands. If conditions warrant, upgrade to a larger memory configuration.

Error Message `TTYDRIVER-2-NOMEM: Unable to allocate [dec] byte status block`

Explanation The async TTY driver was unable to create an internal structure due to a low-memory condition.

Recommended Action Reduce other system activity to ease memory demands. If conditions warrant, upgrade to a larger memory configuration.

VQPCLIENT Messages

This section contains the Dynamic VLAN VQP client error messages.

Error Message `VQPCLIENT-2-CHUNKFAIL: Could not allocate memory for VQP`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `VQPCLIENT-7-DELETING: Freeing deleted saved responses`

Explanation No explanation is available at this time.

Recommended Action No action is required.

Error Message `VQPCLIENT-2-DENY: Host [enet] denied on interface [chars]`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `VQPCLIENT-2-INITFAIL: Platform-specific VQP initialization failed. Quitting`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `VQPCLIENT-2-IPSOCK: Could not obtain IP socket`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `VQPCLIENT-2-PROCFAIL: Could not create process for VQP. Quitting`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `VQPCLIENT-2-SHUTDOWN: Interface [chars] shutdown by VMPS`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `VQPCLIENT-2-TOOMANY: Interface [chars] shutdown by active host limit`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `VQPCLIENT-3-IFNAME: Invalid interface ([chars]) in response`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `VQPCLIENT-3-THROTTLE: Throttling VLAN change on [chars]`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `VQPCLIENT-3-VLANNAME: Invalid VLAN ([chars]) in response`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `VQPCLIENT-4-IPADDR: Main IP address (on [chars]) was deleted`

Explanation No explanation is available at this time.

Recommended Action No action is required.

Error Message `VQPCLIENT-7-NEXTSERV: Trying next VMPS`

Explanation No explanation is available at this time.

Recommended Action No action is required.

Error Message `VQPCLIENT-7-PROBE: Probing primary server [IP_address]`

Explanation No explanation is available at this time.

Recommended Action No action is required.

Error Message `VQPCLIENT-7-RECONF: Reconfirming VMPS responses`

Explanation No explanation is available at this time.

Recommended Action No action is required.

Error Message `VQPCLIENT-7-STARTUP: Starting VQP client`

Explanation No explanation is available at this time.

Recommended Action No action is required.

Error Message `VQPCLIENT-7-STOPPING: Stopping VQP client`

Explanation No explanation is available at this time.

Recommended Action No action is required.

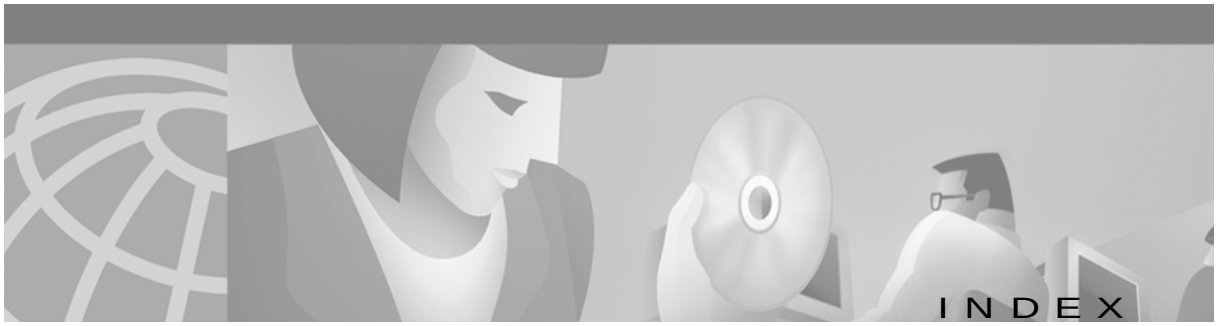
VTP Message

This section contains the Virtual Terminal Protocol error message.

Error Message `VTP-3-ERROR: [chars]`

Explanation No explanation is available at this time.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Enter the **show tech-support** command to gather data that might provide information to determine the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** output, contact your Cisco technical support representative, and provide the representative with the gathered information.



Numerics

1000BASE-T module, Catalyst 2900 XL 1-9
802.1Q trunk mode 2-12

A

aaa (authentication, authorization, and accounting)
  configuring 6-54
  managing 6-51
aaa accounting command 6-54
AAAA system messages A-5
aaa authorization command 6-53
aaa authorization exec tacacs+ local command 6-53
aaa new-model command 6-52, 6-54
abbreviating commands 3-4
abbreviations
  char, variable field A-3
  chars, variable field A-3
  dec, variable field A-3
  hex, variable field A-3
  inet, variable field A-3
AC (command switch) 5-10, 5-21
accessing
  CMS 2-32
    modes 2-33
  command modes 3-2
  console port 4-3
  HTTP port 4-5
  member switches 8-24
accessing (continued)
  MIBs
    files 4-6
    objects 4-5
    variables 4-6
  Telnet access 4-4
access levels, CMS 2-33
access ports
  dynamic 8-5, 8-39
  in switch clusters 5-9
  static 8-5, 8-7
access ports in switch clusters 5-9
accounting in TACACS+ 6-51
adding
  secure addresses 6-18
  static addresses 6-19
  VLAN to database 8-23
address
  count, secure 7-12
  resolution 6-32
  security violations 7-11
  See also addresses
addresses
  dynamic
    accelerated aging 6-34
    aging time 6-16
    default aging 6-34
    described 6-15
    removing 6-16

addresses (continued)
MAC
adding secure 6-18
aging time 6-16
discovering 6-15, 6-32
notification 6-17
tables, managing 6-15
secure
adding 6-18
described 6-15, 6-18
removing 6-18
static
adding 6-19
configuring (EtherChannel) 6-20
described 6-15, 6-19
removing 6-19
Address Resolution Protocol (ARP)
See ARP table
address table
aging time, configuring 6-16
dynamic addresses, removing 6-16
MAC 6-15
maximum number of addresses 6-15
secure addresses
adding 6-18
removing 6-18
static addresses
adding 6-19
removing 6-19
advertisements, VTP 8-11
aging, accelerating 6-34
aging time, changing address 6-16
alarms group, in RMON 4-5
allowed-VLAN list 8-28
AppleTalk Remote Access (ARA) 6-53
Apply button 2-31
ARP table
address resolution 6-32
managing 6-32
ATM ports
duplex and speed 7-2
trunks and other features 8-26
VLAN membership 2-12, 8-5
ATM trunk mode 2-12
authentication
NTP 6-13
TACACS+ 6-51
authorization, TACACS+ 6-51
automatic discovery
adding member switches 5-19
considerations
beyond a non-candidate device 5-7, 5-8
brand new switches 5-9
connectivity 5-4
management VLANs 5-7, 5-8
non-CDP-capable devices 5-6
non-cluster-capable devices 5-6
creating a cluster standby group 5-21
in switch clusters 5-4
See also CDP
automatic recovery, clusters 5-10
See also HSRP
autonegotiation
connecting to devices without 7-2
mismatches 9-3

B

bandwidth, graphs 2-8
BPDU message interval 6-43
broadcast client mode, configuring 6-13
broadcast messages, configuring for 6-13
broadcast storm control
disabling 7-5
enabling 7-4
broadcast traffic and protected ports 7-10
browser configuration 2-1, 4-1, 5-1
buttons, CMS 2-31

C

c2900/c3500 traps 6-49
c2900 traps 6-49
Cancel button 2-31
candidate switch
  adding 5-19
  automatic discovery 5-4
  changing management VLAN for 8-4
  defined 5-3
  HC 5-21
  passwords 5-19
  requirements 5-3
  standby group 5-21
  why not added 9-7
  See also command switch, cluster standby group, and member switch
cascaded configuration, UplinkFast 6-35
Catalyst 3524-PWR XL 7-14
cautions xv
CC (command switch) 5-21
CDP 1-3
  automatic discovery in switch clusters 5-4
  configuring 6-13, 6-14
  system messages A-7
CGMP 1-2
  controlling management packets with 6-20
  removing router ports 6-22
  See also Fast Leave
change notification, CMS 2-34
chassis system messages A-8
Cisco.com xviii
Cisco Access Analog Trunk Gateway 1-14
Cisco Access Digital Trunk Gateway 1-14
Cisco CallManager software 1-12, 1-14
Cisco Discovery Protocol
  See CDP
Cisco Group Management Protocol
  See CGMP
Cisco IP Phones 1-12
Cisco SoftPhone software 1-12
CiscoWorks 2000 1-5, 4-6
Class of service
  See CoS
CLI 1-5
  abbreviating commands 3-4
  accessing 3-7
  basics 3-2
  command modes 3-2
  error messages 3-6
  IOS Release 12.0 documentation xiii
  managing clusters 5-24
  overview 3-1
  saving changes 3-8
  using 3-1
client mode, VTP 8-10
Cluster Management Suite 1-5
  See CMS
Cluster Membership Protocol
  See CMP system messages
clusters, switch
  accessing 5-13
  adding member switches 5-19
  automatic discovery 5-4
  automatic recovery 5-10
  command switch configuration 5-18
  compatibility 5-4
  creating 5-17
  creating a cluster standby group 5-21
  described 5-1
  disqualification code 9-7
  Gigabit Ethernet, illustrated 6-35
  LRE profile considerations 5-17
  management VLAN, changing 8-3
  managing
    through CLI 5-24
    through SNMP 5-25

clusters, switch (continued)
planning considerations
automatic discovery 5-4
automatic recovery 5-10
CLI 5-24
described 5-4
host names 5-14
IP addresses 5-13
LRE profiles 5-17
management VLAN 5-16
NAT commands 5-17
network port 5-16
passwords 5-14
SNMP 5-14, 5-25
switch-specific features 5-17
TACACS+ 5-15
redundancy 5-21
See also candidate switch, command switch, cluster standby group, member switch, and standby command switch
troubleshooting 5-23
verifying 5-23
cluster standby group
automatic recovery 5-11
considerations 5-12
creating 5-21
defined 5-2
requirements 5-3
virtual IP address 5-11
See also HSRP
cluster traps 6-49
cluster tree
described 2-5
icons 2-5
CMP system messages A-8
CMS
accessing 2-32
access levels 2-33
change notification 2-34

CMS (continued)
cluster tree 2-5
described 2-1
different versions of 2-35
displaying system messages 2-21, 9-4, A-1
error checking 2-34
features 2-2
Front Panel images 2-6
Front Panel view 2-4
interaction modes 2-28
menu bar 2-18
online help 2-29
privilege level 2-33, 6-11
requirements 2-32
saving configuration changes 2-34
toolbar 2-23
tool tips 2-29
Topology view 2-13
troubleshooting CMS session 9-4
verifying configuration changes 2-34
window components 2-30
wizards 2-28
Collapse Cluster view 2-14
command-line error messages 3-6
command-line interface
See CLI
command modes 3-2, 3-3
commands
aaa accounting 6-54
aaa authorization 6-53
aaa authorization exec tacacs+ local 6-53
abbreviating 3-4
copy running-config startup-config 9-8
default 3-5
dir flash 9-8
getting help (?) 3-5
help 3-5
list of available 3-3, 3-6
no 3-5

commands (continued)
port block 8-26
redisplaying 3-5
resetting to defaults 3-5
spanning-tree root guard 6-47
stp-list 6-33
undoing 3-5
usage basics 3-2
command switch
active (AC) 5-10, 5-21
and management 4-5
command switch with HSRP disabled (CC) 5-21
configuration conflicts 9-11
defined 5-2
enabling 5-18
passive (PC) 5-10, 5-21
password privilege levels 5-24
priority 5-10
recovery
from failure 9-11, 9-16
from failure without HSRP 9-16
from lost member connectivity 9-11
recovery from command-switch failure 5-10
redundant 5-10, 5-21
replacing
with another switch 9-14
with cluster member 9-12
requirements 5-2
See also candidate switch, cluster standby group, member switch, and standby command switch
standby (SC) 5-10, 5-21
command variables, listing 3-6
community strings
configuring 5-14, 6-49
in clusters 5-14
SNMP 5-14
compatibility, avoiding configuration conflicts 9-2
config traps 6-49
configuration
conflicts, managing 9-2, 9-11
default VLAN 8-20
file, VMPS database 8-36
files, saving to an external server 9-8
guidelines
port 7-2
VLANs 8-20
VMPS 8-37
VTP 8-13
VTP version 8-14
saving to Flash memory 9-8
VTP, default 8-14
configuration changes, saving 2-34, 3-8
configuration examples, network 1-7
collapsed backbone and switch cluster 1-12
design concepts
cost-effective wiring closet 1-8
high-performance workgroup 1-8
network performance 1-7
network services 1-8
redundant Gigabit backbone 1-9
large campus 1-14
multidwelling configuration 1-16
small to medium-sized network 1-10
configuration files, DHCP 6-8
configuring
802.1p class of service 8-30
AAA 6-54
aging time 6-16
broadcast messages 6-13
broadcast storm control 7-4
CDP 6-13, 6-14
community strings 6-49
Cross-stack UplinkFast 6-37
date and time 6-12
daylight saving time 6-12
DNS 6-6

configuring (continued)
duplex 7-2, 7-3
dynamic ports on VMPS clients 8-39
dynamic VLAN membership 8-38
flooding controls 7-4
flow control 7-3
hello time 6-44
hops 6-14
IGMP filtering 6-23
inline power 7-17
IP information 6-2
IP Phone 7-14, 7-15
load sharing 8-32
login authentication 6-52
management VLAN 8-4
native VLANs 8-29
NTP 6-13
passwords 6-11
ports
protected 7-10
privilege levels 6-11
RMON groups 4-5
SNMP 6-48
speed 7-2, 7-3
static addresses (EtherChannel) 6-20
STP 6-33
Cross-stack UplinkFast 6-37
port priorities 8-32
root guard 6-47
UplinkFast 6-35
TACACS+ 6-51
trap managers 6-49
trunk port 8-27
trunks 8-25, 8-27
VLANs 8-1, 8-20, 8-22
VTP 8-13, 8-15
VTP client mode 8-16
VTP server mode 8-15
VTP transparent mode 8-7, 8-17
conflicts, configuration 9-2, 9-11
consistency checks in VTP version 2 8-11
console port
access 4-3
connecting to 3-7
default settings 4-3
conventions
command xv
for examples xv
text xv
copy running-config startup-config command 9-8
CoS
configuring 8-30
priority 7-15
Cross-stack UplinkFast
See CSUF
CSUF 6-37
configuring 6-41
connecting stack ports 6-40
fast convergence causes 6-39
limitations 6-39
overview 6-37
Current Multicast Groups table 6-22

D

database, VTP 8-19, 8-22
date, setting 6-12
daylight saving time 6-12
default configuration
VLANs 8-20
VMPS 8-38
VTP 8-14
defaults, resetting to 3-5
default settings, changing 4-8
deleting VLAN from database 8-24
destination-based forwarding 7-9
destination-based port groups 6-20, 7-8

device icons
Front Panel view 2-5
Topology view 2-15
device labels 2-16
Device Manager 2-2
See also Switch Manager
device pop-up menu
Front Panel view 2-24
Topology view 2-26
DHCP 1-3, 6-3
Client Request Process 6-4
configuring DHCP server 6-5
configuring domain name and DNS 6-6
configuring relay device 6-7
configuring TFTP server 6-5
example configuration 6-9
obtaining configuration files 6-8
overview 6-3
dir flash command 9-8
disabling
broadcast storm control 7-5
CGMP Fast Leave 6-21
network port 7-7
port security 7-12
SNMP 6-48
STP 6-34
Switch Port Analyzer (SPAN) 7-13
trunking on a port 8-28
trunk port 8-28
VTP 8-17
VTP version 2 8-18
discovery, clusters
See automatic discovery
DISL 8-27
display options, Topology view 2-17
disqualification code 9-7
Disqualification Code option 2-27
DNS
configuring 6-6
described 6-6
enabling 6-6
documentation, CD-ROM xvii
documentation, IOS Release 12.0 xiii
documentation, related xvi
domain name
configuring 6-6
described 6-6
specifying 6-6, 8-13
Domain Name System server
See DNS
domains for VLAN management 8-9
DTP 8-27
duplex
configuration guidelines 7-2
configuring 7-2, 7-3
settings, ATM port 7-2
duplex mode LED 2-8
dynamic access mode 2-12
dynamic-access ports
described 8-5
limit on number of hosts 8-41
VLAN membership combinations 8-6
dynamic addresses
See addresses
Dynamic Host Configuration Protocol
See DHCP
Dynamic ISL
See DISL
dynamic ports, configuring 8-39
dynamic port VLAN membership
configuration example 8-41
configuring 8-39
example 8-41
overview 8-35

dynamic port VLAN membership (continued)
reconfirming 8-40
troubleshooting 8-41
VMPS database configuration file 8-36
dynamic port VLAN membership, reconfirming 8-39
Dynamic Trunk Protocol
See DTP
dynamic VLAN membership 8-38
dynamic VLAN VQP client system messages
See
VQPCLIENT system messages A-42

E

egress port scheduling 8-30
enable password
See passwords
enable secret password
See passwords
enabling
broadcast storm control 7-4
CGMP Fast Leave 6-21
DNS 6-6
Fast Leave 6-21
MAC address notification 6-17
network port 7-6
NTP authentication 6-13
Port Fast 6-45
port security 7-11, 7-12
SNMP 6-48
SPAN 7-13
STP Port Fast 6-45
UplinkFast 6-37
VTP pruning 8-18
VTP version 2 8-17
encapsulation 8-30
environment system messages A-9
error checking, CMS 2-34
error messages 3-6
EtherChannel port groups 7-8
configuring static address for 6-20
creating 7-9
Ethernet MANs 1-16
Ethernet VLAN, defaults and ranges 8-20
events group, in RMON 4-5
examples
conventions for xv
network configuration 1-7
Expand Cluster view 2-14
expert mode 2-28
extended discovery 6-14

F

facility codes
description A-2
table A-2
fan fault indication 2-5
Fast EtherChannel port groups, creating 7-8
Fast Ethernet trunks 8-25
Fast Leave
defined 6-20
disabling 6-21
enabling 6-21
FDDI-Net VLAN defaults and ranges 8-21
FDDI VLAN defaults and ranges 8-21
features
configuration conflicts between 7-1, 8-1
conflicting port 9-2
default settings 4-8
incompatible 9-2
IOS 1-1
feedback to Cisco Systems, web xviii
File Transfer Protocol
See FTP, accessing MIB files
Flash memory, files in 9-8
flooded traffic, reducing 7-5
flooding controls, configuring 7-4

flow control, configuring 7-3
forwarding
  delay 6-42, 6-44
  port groups 7-8
  restrictions 7-9
  resuming 7-6
  source-based, illustrated 7-8
  See also broadcast storm control
forwarding, static address 6-19
Frank system messages A-10
Front Panel images, CMS 2-6
Front Panel view
  cluster tree 2-5
  described 2-4
  pop-up menus 2-24
  port icons 2-6
  port LEDs 2-8
  RPS LED 2-7
  switch images 2-6
FTP, accessing MIB files 4-6

G

GBIC_1000BASET system messages A-15
GBICs
  1000BASE-LX/LH module 1-8
  1000BASE-SX module 1-8
  1000BASE-T module 1-9
  1000BASE-ZX module 1-9
  GigaStack 1-8
get-next-request operation 4-6, 4-7
get-request operation 4-6, 4-7
get-response operation 4-7
Gigabit Ethernet
  clusters, illustrated 6-35
  ports, configuring flow control on 7-3
  port settings 7-2
  settings 7-2
  trunks 8-25
Gigabit Interface Converter
  See GBICs
GigaStack system messages A-16
global configuration mode 3-3
graphs
  bandwidth 2-8
  poll result 4-6
guide mode 1-6, 2-28

H

hardware memory system messages
  See HW_MEMORY system messages
HC (candidate switch) 5-21
hello BPDU interval 6-44
hello time
  changing 6-44
  defined 6-42
help, CLI 3-5
Help button, CMS 2-31
Help Contents 2-29
history group, in RMON 4-5
hold-time, modifying 6-22
hops, configuring 6-14
host name list, CMS 2-30
host names
  abbreviations appended to 5-21
  in clusters 5-14
  to address mappings 6-6
hosts, limit on dynamic ports 8-41
HP OpenView 1-5
HSRP
  automatic cluster recovery 5-11
  cluster standby group considerations 5-12
  recovering from command switch failure 9-11
  See also clusters, cluster standby group, and standby command switch
hsrp traps 6-49
HTTP access 2-32, 4-5

HW_MEMORY system messages A-17
Hypertext Transfer Protocol
See HTTP access

I

icons
cluster tree 2-5
colors
cluster tree 2-5
Topology view 2-17
editable table cell 2-31
Front Panel view 2-6
multilink 2-25
sorting 2-31
toolbar 2-23
Topology view 2-15
web link 2-31
IEEE 802.1P 7-14
IEEE 802.1Q
configuration considerations 8-25
interaction with other features 8-26
native VLAN for untagged traffic 8-29
overview 8-25
IEEE 802.1Q trunks 8-25
IGMP filtering 1-2
applying filters 6-25
configuring 6-23
groups 6-26
profiles 6-23
ingress port scheduling 8-30
inline power, configuring 7-17
inline power LED 2-11
inline power port mode LED 2-8
interaction modes, CMS 2-28
interface API system messages A-18
interface configuration mode 3-3
specifying ports in 3-4
interfaces, IOS supported 1-5
Internet Group Management Protocol
See IGMP filtering
Internet Protocol system messages
See IP
Inter-Switch Link
See ISL
inventory, cluster 5-23
IOS command-line interface
See CLI
IOS Release 12.0 documentation xiii
IP addresses
candidate or member 5-3, 5-13
cluster access 5-2
command switch 5-2, 5-11, 5-13
discovering 6-32
management VLAN 5-16, 8-3
redundant clusters 5-11
removing 6-2
standby command switch 5-11, 5-13
See also IP information
IP connectivity to the switch 4-2
ip igmp profile command 6-23
IP information
assigning 6-2
configuring 6-2
removing 6-2
IP management packets, controlling 6-20
IP Phone
calls 7-14
configuring 7-14, 7-15
sound quality 7-14
IP system messages A-18
IPX server time-out, and Port Fast 6-45
ISL 1-4
interaction with other features 8-26
overview 8-25
ISL trunk mode 2-12

J

Java plug-in configuration 2-1, 4-1, 5-1

L

LEDs
duplex mode 2-8
LINE PWR mode 2-8
LRE mode 2-8
port 2-8
port (Catalyst 2900 LRE XL) 2-10
port (Catalyst 2900 XL, except Catalyst 2900 LRE XL) 2-9
port (Catalyst 3500 XL) 2-11
port modes 2-8
RPS 2-7
RPS 300 2-7
RPS 600 2-7
speed mode 2-8
STAT mode 2-8
legend, CMS icons and labels 2-22
line configuration mode 3-3
LINE PWR mode LED 2-11
link icons, Topology view 2-16
link labels 2-16
link pop-up menu, Topology view 2-25
lists, CMS 2-31
load sharing
STP, described 8-31
using STP path cost 8-33
using STP port priorities 8-31
login authentication, configuring 6-52
Long-Reach Ethernet (LRE) technology xiii, 1-1
LRE mode LED 2-8

M

MAC addresses
adding secure 6-18
aging time 6-16
discovering 6-15, 6-32
maximum number supported 6-15
notification and history of activity 6-17
MAC address notification feature 1-4
MAC address tables, managing 6-15
mac-notification traps 6-49
management options 1-5
benefits
clustering 1-6
CMS 1-6
CLI 3-1
CMS 2-1
management VLAN
changes, understanding 8-3
changing 5-16, 8-3, 8-4
configuring 8-4
IP address 5-16, 8-3
switch clusters 5-16
considerations in clusters 5-7, 5-8
MANs, Ethernet 1-16
map
See topology
membership mode, VLAN port 2-12, 8-5
member switch
adding 5-19
automatic discovery 5-4
defined 5-2
managing 5-24
passwords 5-13
requirements 5-3
See also candidate switch, cluster standby group, and standby command switch

member switches
accessing 8-24
recovering from lost connectivity 9-11
menu bar
described 2-18
variations 2-18
messages
CLI error 3-6
system 2-21, 9-4, A-1
message severity levels
description A-3
table A-3
MIBs, accessing
files 4-6
objects 4-5
variables 4-6
mini-point-of-presence
See POP
mirror system messages A-20
mismatches, autonegotiation 9-3
mnemonic code A-3
Mode button 2-8
modes
access to CMS 2-33
command 3-2
port 2-8
VLAN port membership 2-12, 8-5
VTP
See VTP modes
Modify button 2-31
module system messages A-20
monitoring
ports 7-13
traffic 7-13
VMPS 8-41
VTP 8-19
multicast groups
described 6-20
removing 6-22
multicast packets
See flooding controls
multicast traffic and protected ports 7-10
Multicast VLAN Registration
See MVR
Multilink Decomposer window 2-25
multilink icon 2-25
multi-VLAN mode 2-12
multi-VLAN ports
assigning to VLANs 8-7, 8-8
described 8-7
VLAN membership combinations 8-6
MVR 6-27
configuring 6-31
guidelines 6-29
limitations 6-29
overview 6-27
parameters 6-30

N

NAT commands, cluster considerations 5-17
native VLANs 8-29
NCPs 6-53
neighboring devices, types of 2-15
Network Address Translation
See NAT commands
network configuration examples 1-7
Network Control Protocols (NCPs) 6-53
network examples 1-7
collapsed backbone and switch cluster 1-12
design concepts
cost-effective wiring closet 1-8
high-performance workgroup 1-8
network performance 1-7
network services 1-8
redundant Gigabit backbone 1-9

network examples 1-7 (continued)
large campus 1-14
multidwelling configuration 1-16
small to medium-sized network 1-10
Network Management System
See NMS
network ports
disabling 7-7
enabling 7-6
switch clusters 5-16
and trunks 8-26
Network Time Protocol
See NTP
NMS 4-6
no commands, using 3-5
notification, MAC address 1-4, 6-17
NTP
authentication 6-13
broadcast-client mode 6-13
client 6-13
configuring 6-13
described 6-13

O

OK button 2-31
online help 2-29
operating system messages
See SYS system messages A-37
overheating indication, switch 2-5

P

packets 7-5
controlling management (CGMP) 6-20
See also traffic
parallel links 8-31
passwords
changing 6-11
community strings 6-49
in clusters 5-14, 5-19
in CMS 2-32
recovery of 9-16, 9-17
setting 6-11
TACACS+ server 6-51
VTP domain 8-13
path cost 6-45, 6-46, 8-33
PC (passive command switch) 5-10, 5-21
PERF5_HALT_MSG (manufacturing test) system messages A-21
planning considerations, switch clusters
LRE profiles 5-17
management VLAN 5-16
NAT commands 5-17
network port 5-16
switch-specific features 5-17
poll results, graphing 4-6
POP 1-16
port block command 7-10, 8-26
Port Fast
enabling 6-45
STP parameter 8-37
port groups
and trunks 8-26
configuring static addresses (EtherChannel) 6-20
creating EtherChannel 7-8, 7-9
destination-based 6-20, 7-8
forwarding 7-8
restrictions on forwarding 7-9
source-based 6-20, 7-8
See also ports
port icons, Front Panel view 2-6

port LEDs
Catalyst 2900 LRE XL 2-10
Catalyst 2900 XL, except Catalyst 2900 LRE XL 2-9
Catalyst 3500 XL 2-11
port modes 2-8
Port Manager state machine system messages
See PMSM system messages
Port Manager system messages
See PM system messages
port membership modes, VLAN 2-12, 8-5
port modes
described 2-8
LEDs 2-8
port-monitoring conflicts with trunks 8-26
port number 3-4
port pop-up menu, Front Panel view 2-24
ports
802.1Q trunk 2-12
ATM
duplex and speed 7-2
trunks and other features 8-26
VLAN membership 2-12, 8-5
ATM trunk 2-12
configuration guidelines 7-2
configuring
protected 7-10
trunk 8-27
dynamic
configuring 8-39
See also dynamic port VLAN membership
dynamic access 2-12
hosts on 8-41
mode 8-5
and VLAN combinations 8-6
dynamic VLAN membership, reconfirming 8-39
features, conflicting 9-2
flooded traffic 7-5
forwarding, resuming 7-6

ports (continued)
Gigabit Ethernet
configuring flow control on 7-3
settings 7-2
ISL trunk 2-12
monitoring 8-26
multi-VLAN 2-12, 8-5, 8-7, 8-8
network 8-26
priority 6-46, 8-30, 8-31
protected 7-10
secure 7-12, 8-26
security
described 7-11
disabling 7-12
enabling 7-12
specifying in interface configuration mode 3-4
speed, setting and checking 7-2
static-access 2-12, 8-5, 8-6, 8-7, 8-24
STP states 6-45
trunk
configuring 8-27
disabling 8-28
trunks 8-5, 8-25
VLAN assignments 8-7, 8-24
See also port groups
port scheduling 8-30
port security 1-4
port security system messages A-25
power, inline 7-17
power detection on the Catalyst 3524-PWR 7-17
priority
modifying switch 6-43
overriding 7-15
port
described 8-30
modifying 6-45, 6-46
private VLAN edge ports
See protected ports
privileged EXEC mode 3-3

privilege levels
access modes
read-only 2-33
read-write 2-33
CMS 2-33
command switch 5-24
mapping on member switches 5-24
setting 6-11
specifying 6-12
protected ports 1-2, 7-10
pruning
enabling on a port 8-29
enabling on the switch 8-18
overview 8-12
pruning-eligible list 8-29
PSTN 1-14
publications, related xvi

Q

QoS
egress port scheduling 8-30
ingress port scheduling 8-30, 8-31

R

RAC system messages A-29
rcommand command 5-24
read-only access mode 2-33
read-write access mode 2-33
reconfirmation interval, changing 8-40
recovery procedures 9-11
redisplaying commands 3-5
redundancy
STP 6-34
path cost 8-33
port priority 8-31
UplinkFast 6-36
redundant clusters
See cluster standby group
redundant power system
See RPS
Refresh button 2-31
registors system messages A-29
relay device, configuring 6-7
releases, switch software 4-2
remote devices without autonegotiation, connecting to 7-2
remote monitoring
See RMON
remove vlan-list parameter 8-28
removing
dynamic address entries 6-16
IP information 6-2
multicast groups 6-22
secure addresses 6-18
static addresses 6-19
retry count, changing 8-40
RFC
1157, SNMPv1 6-48
1901, SNMPv2C 6-48
1902 to 1907, SNMPv2 6-48
RMON, supported groups 4-5
root guard 6-47
router autoconfiguration system messages
See RAC system messages A-29
router hold-time, modifying 6-22
RPS LED
RPS 300 2-7
RPS 600 2-7
RTD messages A-30
Runtime Diagnostic
See RTD messages

S

saving changes in CMS 2-34
SC (standby command switch) 5-10, 5-21
secure address count 7-12
secure addresses
  adding 6-18
  described 6-18
  removing 6-18
secure ports
  address-security violations 7-11
  disabling 7-12
  enabling 7-11, 7-12
  maximum secure address count 7-12
  and trunks 8-26
security
  port 7-11
  TACACS+ 6-51
  violations, address 7-11
Serial Line Internet Protocol
  See SLIP
server, domain name 6-6
server mode, VTP 8-10
servers, BOOTP 1-3, 6-3
set-request operation 4-6, 4-7
settings
  default, changing 4-8
  duplex 7-2, 7-3
  Gigabit Ethernet port 7-2
  speed 7-3
  STP 6-35
  STP default 6-35
severity levels
  description A-3
  table A-3
show cluster members command 5-24
Simple Network Management Protocol
  See SNMP
SLIP 6-53
SNMP
  accessing MIB variables with 4-6
  community strings, configuring 6-49
  configuring for single switches 6-48
  enabling and disabling 6-48
  in-band management 1-3
  in clusters 5-14
  management, using 4-5
  managing clusters with 5-25
  network management platforms 4-5
  RMON groups 4-5
  system messages A-31
  trap managers, configuring 6-49
  trap types 6-49, 6-50
snmp traps 6-49
  c2900 6-49
  c2900/c3500 6-49
  cluster 6-49
  config 6-49
  hsrp 6-49
  mac-notification 6-49
  snmp 6-49
  tty 6-49
  vlan membership 6-49
  vtp 6-49
software
  recovery procedures 9-19
  requirements for changing management VLAN 5-16
  VLAN considerations 8-13
  See also upgrading
software releases 4-2
source-based forwarding 7-9
source-based port groups 6-20, 7-8
SPAN 7-13
  disabling 7-13
  enabling 7-13
  ports, restrictions 9-2
Spanning Tree Protocol
  See STP

spanning-tree rootguard command 6-47
speed, setting 7-2, 7-3
speed mode LED 2-8
Standby Command Configuration window 5-22
standby command switch
  configuring 5-21
  considerations 5-12
  defined 5-2
  priority 5-10
  requirements 5-3
  virtual IP address 5-11
  See also cluster standby group and HSRP
standby group, cluster
  See cluster standby group and HSRP
static access mode 2-12
static-access ports
  assigning to VLAN 8-7, 8-24
  described 8-7
  VLAN membership combinations 8-6
static addresses
  adding 6-19
  configuring for EtherChannel port groups 6-20
  described 6-15, 6-19
  removing 6-19
  See also static address
static address forwarding 6-19
static address forwarding restrictions 7-9
statistics, VTP 8-19
statistics group, in RMON 4-5
STAT mode LED 2-8
storm control system messages A-35
STP
  behavior, unpredictable 8-8
  BPDU message interval 6-43
  configuring 6-33, 6-35
  disabling 6-34

STP (continued)
  forwarding delay timer 6-44
  hello BPDU interval 6-44
  implementation type 6-42
  load sharing
    overview 8-31
    using path costs 8-33
    using port priorities 8-31
  parameters 6-33
  path cost
    changing 6-46
    configuring 8-33
  Port Fast
    enabling 6-45
    mode 8-37
  port grouping parameters 7-8, 8-26
  port priority 6-46, 8-32
  port states 6-45
  redundant connectivity 6-34
  redundant links with UplinkFast 6-36
  root guard 6-47
  settings 6-35
  STP implementation, changing 6-42
  STP instances
    considerations 6-33
    maximum number supported 6-33
  supported number of spanning-tree instances 6-33
  switch priority 6-43
  UplinkFast 6-36, 6-37
  VLAN parameters described 6-42
STP fast convergence system messages
  See SPANTREE_FAST system messages A-34
stp-list parameter 6-33
STP port states 6-45
STP system messages
  See SPANTREE system messages A-31

SunNet Manager 1-5
switch clustering technology 5-1
switch clusters
  planning considerations
    LRE profiles 5-17
    management VLAN 5-16
    NAT commands 5-17
    network port 5-16
    switch-specific features 5-17
  troubleshooting 9-7
Switch Manager 2-2, 2-35
  See also Device Manager
Switch Port Analyzer
  See SPAN
switchport command 8-27
switch ports, configuring 7-1
switch software releases 4-2
switch upgrades, troubleshooting 9-9
system date and time 6-12
system messages 2-21, 9-4, A-1
  AAAA A-5
  CDP A-7
  chassis A-8
  CMP A-8
  environment A-9
  Frank A-10
  GBIC_1000BASET A-15
  GigaStack A-16
  how to read A-2
  HW_MEMORY A-17
  interface API A-18
  IP A-18
  list of A-4
  mirror A-20
  module A-20
  on CMS 2-21, 9-4, A-1
  PERF5_HALT_MSG A-21
  PM A-22
  PMSM A-24
system messages 2-21, 9-4, A-1 (continued)
  port security A-25
  pruning A-25
  RAC A-29
  recovery procedures A-4
  registors A-29
  RTD A-30
  SNMP A-31
  SPANTREE A-31
  SPANTREE_FAST A-34
  storm control A-35
  SW_VLAN A-35
  SYS A-37
  TAC A-40
  traceback reports A-4
  TTYDRIVER A-41
  VTP A-45

T

tables
  message severity levels A-3
  variable fields A-3
tables, CMS 2-31
tabs, CMS 2-31
TACACS+
  AAA accounting commands 6-54
  AAA authorization commands 6-53
  configuring 6-51
  in clusters 5-15
  initializing 6-52
  server, creating 6-51
  starting accounting 6-54
TACACS+ authentication, authorization, and accounting security system messages
  See AAAA system messages A-5
tacacs-server host command 6-51, 6-52
tacacs-server retransmit command 6-52, 6-54
tacacs-server timeout command 6-52

TACACS system messages
See TAC system messages
Telnet
access 4-4
accessing management interfaces 3-7
accessing the CLI 1-5
from a browser 3-7
terminal driver system messages
See TTYDRIVER system messages A-41
TFTP server, configuring 6-5
time
daylight saving 6-12
setting 6-12
zones 6-12
TLV support 8-11
Token Ring VLANs
overview 8-19
TRBRF 8-11, 8-21
TRCRF 8-11, 8-22
toolbar 2-23
tool tips 2-29
Topology view
Collapse Cluster view 2-14
described 2-13
device icons 2-15
colors 2-17
device labels 2-16
display options 2-17
Expand Cluster view 2-14
icons 2-15
link icons 2-16
link labels 2-16
multilink icon 2-25
neighboring devices 2-15
pop-up menus 2-25
troubleshooting 9-7
traceback reports A-4
traffic
blocking flooded 7-5
forwarding, and protected ports 7-10
monitoring 7-13
reducing flooded 7-4, 7-6
transmit queue 8-30
transparent mode, VTP 8-10, 8-17
trap managers
adding 6-49
configuring 6-49
traps 4-7
traps, snmp
c2900 6-49
c2900/c3500 6-49
cluster 6-49
config 6-49
hsrp 6-49
mac-notification 6-49
snmp 6-49
tty 6-49
vlan membership 6-49
vtp 6-49
TRBRF VLAN defaults and ranges 8-21
TRCRF VLAN defaults and ranges 8-22
troubleshooting 9-1
autonegotiation mismatches 9-3
CMS sessions 9-4
configuration conflicts 9-2
recovery procedures for 9-11
switch clusters 9-7
switch upgrades 9-9
using configuration files 9-8
with CiscoWorks2000 4-6
trunk ports
configuring 8-27
disabling 8-28

trunks
allowed-VLAN list 8-28
ATM 8-26
blocking unknown packets on 8-26
configuration conflicts 8-26
configuring 8-27
disabling 8-28
Gigabit Ethernet 8-25
IEEE 802.1Q 8-25
interacting with other features 8-26
ISL 8-25
load sharing using
STP path costs 8-33
STP port priorities 8-31
native VLAN for untagged traffic 8-29
overview 8-25
parallel 8-33
pruning-eligible list 8-29
VLAN, overview 8-25
VLAN membership combinations 8-6
tty traps 6-49

U

UDLD 7-7
unicast and multicast packets, unknown
See flooding controls
unicast traffic and protected ports 7-10
UniDirectional Link Detection
See UDLD
Unrecognized Type-Length-Value
See TLV support
upgrading software 4-1
VLAN considerations 8-13
UplinkFast
configuring 6-35
enabling 6-37
redundant links 6-36
URLs, Cisco xvii
user EXEC mode 3-3

V

variable fields
definition A-3
table A-3
verifying changes in CMS 2-34
version-dependent transparent mode 8-11
virtual IP address
cluster standby group 5-11, 5-21
command switch 5-11, 5-21
See also IP addresses
Virtual Terminal Protocol system messages
See VTP system messages
VLAN
adding to database 8-23
modifying 8-23
port membership modes 2-12, 8-5
trunks
overview 8-25
support on older switches and software 8-3
VLAN database mode 3-3
VLAN ID, discovering 6-15, 6-32
VLAN Management Policy Server
See VMPS
VLAN Manager system messages
See SW_VLAN system messages A-35
VLAN membership
ATM port 8-5
combinations 8-6
confirming 8-39
modes 2-12, 8-5
port group parameters 7-8
See also dynamic VLAN membership
vlan membership traps 6-49

VLAN Query Protocol
See VQP
VLANs
802.1Q considerations 8-25
adding to database 8-23
aging dynamic addresses 6-34
allowed on trunk 8-28
changing 8-23
configuration guidelines 8-20
configuring 8-1, 8-22
default configuration 8-20
deleting from database 8-24
described 8-2
illustrated 8-2
ISL 8-25
MAC addresses 6-15
maximum number supported 8-2
modifying 8-23
multi-VLAN ports 8-7, 8-8
native, configuring 8-29
number supported 8-2
overlapping 8-7
overview 8-2
static-access ports 8-7, 8-23, 8-24
STP instances 8-2
STP parameters, changing 6-42
supported VLANs 8-2
Token Ring 8-19
trunking 8-3
trunks configured with other features 8-26
See also trunks
VTP database and 8-19
VTP modes 8-10
See also management VLAN
VLAN Trunking Protocol
See VTP
VMPS
administering 8-41
configuration guidelines 8-37
database configuration file example 8-36
default configuration 8-38
dynamic port membership
configuring 8-39
example 8-41
overview 8-35
reconfirming 8-39, 8-40
troubleshooting 8-41
mapping MAC addresses to VLANs 8-35
monitoring 8-41
overview 8-35
reconfirmation interval, changing 8-40
reconfirming membership 8-39
retry count, changing 8-40
server address, entering on client 8-38
Voice-over-IP
configuring 7-14
port configuration 7-15
voice ports, configuring 7-14, 7-16
voice traffic 7-17
voice VLAN
See VVID
VQP 8-35
VQPCLIENT A-42
VTP 1-4
advertisements 8-11
configuration guidelines 8-13
configuring 8-15
consistency checks 8-11
database 8-19, 8-22
default configuration 8-14
described 8-9
disabling 8-17

VTP 1-4 (continued)
domain names 8-13
domains 8-9
modes
client 8-10
configurations affecting mode changes 8-10
configuring 8-16
server 8-10, 8-15
transitions 8-10
transparent 8-7, 8-10, 8-17
monitoring 8-19
pruning
enabling 8-18
overview 8-12
pruning-eligible list, changing 8-29
statistics 8-19
Token Ring support 8-11
transparent mode, configuring 8-17
using 8-9
version, determining 8-14
version 1 8-11
version 2
configuration guidelines 8-14
disabling 8-18
enabling 8-17
overview 8-11
VLAN parameters 8-19
VTP pruning system messages
See pruning system messages
vtp traps 6-49
VVID 1-4, 7-14
configuring 7-16

W

warnings xv
web-based management software
See CMS
window components, CMS 2-30
wizards 1-6, 2-28

X

Xmodem protocol 9-19